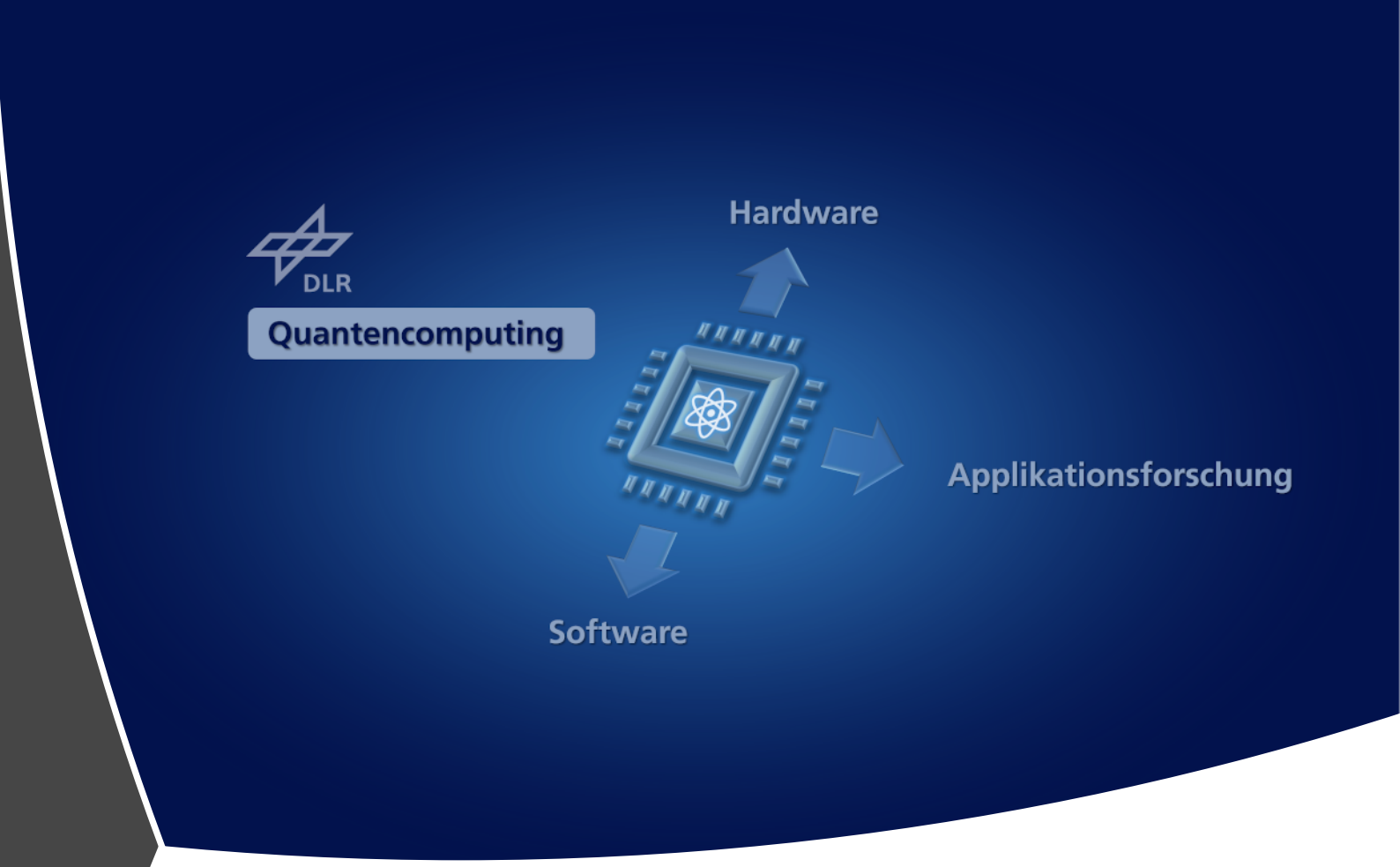

Umfeldstudie Quantencomputing

Tobias Stollenwerk

DLR

Autor	Tobias Stollenwerk
	Deutsches Zentrum für Luft- und Raumfahrt
	Institut für Softwaretechnologie
	Abteilung High-Performance Computing
Adresse	Linder Höhe
	51147 Köln
Telefon	+49 2203 601-4199
E-Mail	tobias.stollenwerk@dlr.de

Version	304ff3, 27. Mai 2021

Inhaltsverzeichnis

1 Einleitung

Quantencomputer sind eine neuartige Form von Hochleistungsrechnern. Sie unterscheiden sich in ihrer Funktionsweise fundamental von klassischen Computern. Während klassische Computer die Informationen in Bits mit zwei diskreten Zuständen speichern, verwenden Quantencomputer sogenannte Quantenbits (kurz Qubits), welche sich als kontinuierliche Überlagerung von zwei Zuständen beschreiben lassen. Dadurch ist es im Prinzip möglich, exponentiell mehr Informationen in einem Register aus Quantenbits zu speichern als in einem Register aus klassischen Bits. Im Gegensatz zu klassischen Computern, die sich durch rein klassische Physik beschreiben lassen, werden in einem Quantencomputer quantenphysikalische Prozesse ausgenutzt, um in Qubits gespeicherte Informationen zu manipulieren. Insbesondere quantenphysikalische Effekte wie Superposition und Verschränkung können ausgenutzt werden, um Informationen parallel zu verarbeiten und unter Umständen exponentielle Laufzeitverbesserungen zu erreichen [Sho94].

Nachdem Quantencomputer in den 1980er Jahren als theoretisches Konzept erfunden wurden [Fey86], gab es in den 1990er Jahren entscheidende Fortschritte in der Entwicklung von Algorithmen für Quantencomputer [DJ92; Sho94; Gro96]. Jedoch erst die beeindruckende Hardwareentwicklung der letzten Jahre haben dem Gebiet eine weitreichende Aufmerksamkeit beschert. Heute scheint das Ziel, eine Laufzeitverbesserungen für eine nützliche Anwendung auf einem Quantencomputer zu demonstrieren, in greifbarer Nähe.

Diese Studie hat das Ziel, dem Leser einen Überblick über die aktuelle Situation der technologischen Entwicklungen im Bereich Quantencomputer zu verschaffen. Der Fokus liegt dabei auf der Anwendungsrelevanz der Technologie sowie auf der deutschen Forschungs- und Industrielandschaft. Insbesondere für die Beleuchtung der Hardwareentwicklungen greifen wir dabei auf Erkenntnisse von ähnlichen Studien mit anderem Fokus, wie die BSI-Studie [Wil+20] und die Studie der Deutschen Akademie der Wissenschaften [Kag+20], zurück.

Die Studie ist wie folgt aufgebaut. Zunächst werden die Grundlagen des Quantencomputing in Kapitel 2 vorgestellt, bevor die verschiedenen Hardwareansätze in Kapitel 3 diskutiert werden. Anschließend behandeln wir die aussichtsreichsten Quantenalgorithmen und

Anwendungsbereiche in Kapitel 4. Mit diesem Wissen ausgestattet, beschäftigen wir uns in Kapitel 5 mit der Rolle des DLR und deutscher Unternehmen im Umfeld nationaler und internationaler Akteure.

2 Grundlagen

In diesem Kapitel behandeln wir die Grundlagen des Quantencomputings. Insbesondere führen wir die Begriffe ein, welche für die folgenden Kapitel 3 und 4 benötigt werden.

2.1 Gattermodell

In jedem Quantencomputer werden die Information in einem **Quantenregister**, bestehend aus einer Reihe von Qubits, gespeichert. Die Berechnung besteht in der Manipulation des Quantenregisters. Im sogenannten **Gattermodell** besteht diese Manipulation aus unitären Operationen, die auf ein einzelnes oder mehrere Qubits wirken (*n*-**Qubitgatter**). Unitär bedeutet in diesem Zusammenhang, dass die Information zwar manipuliert werden kann, aber grundsätzlich erhalten bleibt. Eine Menge von Gatteroperationen heißt **universell**, wenn sich durch Kombination ihrer Elemente jede unitäre Operation realisieren lässt. Stehen solche Gatteroperationen zur Verfügung, spricht man folglich von einem **universellem Quantencomputer**.

Ein **Quantenalgorithmus** besteht nun aus einer Abfolge von Gattern, welche das Quantenregister von einem Anfangs- in einen Endzustand überführt. Dieser Endzustand wird anschließend ausgelesen. Aufgrund der statistischen Natur des quantenmechanischen Messprozesses wird dieser Vorgang üblicherweise mehrmals wiederholt. Beispiele für solche Quantenalgorithmen sind die Algorithmen von Shor [Sho94] und Grover [Gro96].

Im Gegensatz zu dem oben beschriebenen Bild werden echte Quantencomputer immer fehlerbehaftet sein. Diese Fehler können vielgestaltig sein. Zum einen gibt es **kohärente Fehler**, welche man sich zum Beispiel als Über- oder Unterrotation auf der Blochkugel vorstellen kann. Obwohl diese Fehler den Algorithmus verfälschen, erhalten sie die Unitärität und damit die Informationen im Quantenregister. Im Gegensatz dazu kommt es bei **dekohärenten Fehlern** zu einem Informationsverlust im Quantenregister. Die Zeitskala, auf der solche dekohärenten Fehler wirken, wird als **Dekohärenzzeit** bezeichnet.

Es ist prinzipiell möglich, solche Fehler – sofern sie klein sind – zu korrigieren. Im Gegensatz zu klassischen Systemen ist es in Quantencomputern jedoch nicht möglich, dies über multiple Kopien der Qubitinformationen zu erreichen. Ein fundamentales Theorem der Quantentheorie, das *No-Cloning* Theorem, verbietet dies. Stattdessen funktioniert die **Quantenfehlerkorrektur** wie folgt: Einzelne logischen Qubits werden auf mehrere physikalische Qubits verteilt [NC11]. Obwohl die Effizienz solcher Strategien durch die Einführung der sogenannten *Surface Code* Methode signifikant gesteigert wurde, wird immer noch eine große Zahl an zusätzlichen Ressourcen, in Form von Gattern und Qubits, für die Umsetzung benötigt. Durch die Methode der Quantenfehlerkorrektur kann ein fehlerbehafteter Quantencomputer im Prinzip einen idealen, fehlerfreien Quantencomputer simulieren.

2.2 Ära der fehlerbehafteten Quantencomputer (NISQ)

Die Quantencomputer, welche kurz und mittelfristig realisierbar sind, werden keine Algorithmen mit Quantenfehlerkorrektur ausführen können, da einerseits die Fehlerraten noch zu groß sind und andererseits zu wenige Qubits zur Verfügung stehen. Solche Maschinen werden als ***Noisy-Intermediate-Scale-Quantum*** **(NISQ)**-Computer bezeichnet. Für NISQ-Computer sind bis jetzt keine Algorithmen bekannt, die eine garantierte Laufzeitverbesserung gegenüber klassischen Computern besitzen. Man hofft jedoch, mit sogenannten Quantenheuristiken eine Überlegenheit gegenüber herkömmlichen Algorithmen zu demonstrieren. Dabei handelt es sich oftmals um Algorithmen, bei denen es Hinweise, jedoch keine Beweise, für eine Laufzeitverbesserung gibt. Viele dieser Algorithmen kommen ohne Quantenfehlerkorrektur aus und sind somit auf NISQ-Computern ausführbar. Trotzdem ist eine genaue Kenntnis der Fehler für die Entwicklung geeigneter NISQ-Algorithmen notwendig. Um eine nützliche Anwendung auf einem Quantencomputer schneller als auf einem klassischen Computer umzusetzen, bedarf es daher der engen Zusammenarbeit von Hard- und Softwareentwicklern. Nur so können die Kennzahlen und Fehlermodelle der echten Maschinen in die Algorithmenentwicklung einbezogen werden und andererseits Hardwareentwickler genau die Ziele umsetzten, welche in Hinblick auf Algorithmen und mögliche Anwendungen am vielversprechendsten sind. Dieses Vorgehen wird als **Hardware-Software-Codesign** bezeichnet.

2.3 Quantenannealing

Neben dem Gattermodel für Quantencomputer nehmen sogenannte Quantenannealer eine Sonderrolle ein. Das zugrundeliegende Rechenmodel solcher Maschinen wird als **adiabatisches Quantencomputing** [KN98; Far+00] bezeichnet. Im Gegensatz zum Quantenannealing wird hierbei von einem System ohne Fehler im Temperaturnullpunkt ausgegangen. Obwohl ein universeller Quantencomputer theoretisch durch einen adiabatischen Quantencomputer simuliert werden kann, sind Quantenannealer praktisch auf das Lösen von kombinatorischen Optimierungsproblemen sowie die Stichprobennahme für Modelle des maschinellen Lernens beschränkt. Für beide Anwendungen werden niederenergetische Zustände einer pseudo-Boolschen Funktion (eine Funktion, die von binären Variablen abhängt) berechnet. Hier wird der gewünschte Endzustand im Gegensatz zum Gattermodell nicht durch eine Sequenz von Quantengattern erreicht sondern durch die kontinuierliche Veränderung der äußeren Einwirkung auf das Quantenregister. Zuletzt ist die Energie des Systems als Funktion der Bitzustände gerade die pseudo-Boolsche Funktion. Falls sich das Quantenregister zu Anfang im niedrigsten Energiezustand befindet und die Veränderung hinreichend langsam erfolgt, garantiert das adiabatische Theorem aus der Physik, dass sich das Quantenregister in einem Endzustand befindet, der dem Minimum der pseudo-Boolschen Funktion entspricht. Ob es eine Laufzeitverbesserung gegenüber klassischen Verfahren gibt, ist Gegenstand aktueller Forschung. Es wird jedoch davon ausgegangen, dass eine mögliche Laufzeitverbesserung bestenfalls polynomiell ist [Den+16].

2.4 Weitere Ansätze und Varianten

Neben den bereits erwähnten Ansätzen möchten wir noch zwei neuere und exotische Ansätze aufzählen. Erstens ist dies **Continuous-Variable Quantum Computing** [LB99]. Zur Informationsspeicherung werden hier Quantensysteme betrachtet, deren Zustände kontinuierliche Werte annehmen können (im Gegensatz zu den zwei diskreten Werten im Gattermodell). Dieses Konzept ist sehr interessant, da die Herstellung einer Vielzahl von verschränkten Quantenmoden zur Speicherung von Informationen bereits demonstriert wurde [Pfi19] und damit die Umsetzung großskaliger Systeme möglich erscheint. Im Vergleich zu diskretem Quantencomputing ist es jedoch viel schwieriger, Fehler zu korrigieren. Daher erscheint eine Umsetzung solcher Systeme noch nicht in Reichweite.

Des Weiteren möchten wir hier das **One-Way Quantum Qomputing** [RBB03], oder **Measurement-Based Quantum Computing**, ansprechen. Hierbei wird zunächst ein spezieller verschränkter Quantenzustand erzeugt. Anschließend werden Messungen an nur

einem Qubit vorgenommen. Es kann gezeigt werden, dass dieser Ansatz äquivalent zum Gattermodell ist. Die Funktionsweise ist jedoch sehr verschieden. Daher befindet sich die Hardwareentwicklung einerseits noch in einem frühen Stadium, andererseits könnten sich völlig neuartige Wege zur Umsetzung ergeben.

3 Hardwareplattformen

In diesem Kapitel beleuchten wir die verschiedenen Ansätze für Quantencomputerhardware und bewerten diese in Bezug auf ihre mögliche Anwendbarkeit. Dabei orientieren wir uns sehr stark an der BSI-Studie [Wil+20]. Im Gegensatz zu der vorliegenden Studie, die sich in kleinem Umfang mit einer großen Zahl von Anwendungen befasst, ist der Umfang der BSI-Studie um ein vielfaches größer und es wurde ein starker Fokus auf Kryptoanalyse als Anwendung gesetzt.

Das Kapitel ist wie folgt aufgebaut: Nach einer kurzen Übersicht werden die Leistungsindikatoren für Hardwareplattformen eingeführt. Anschließend stellen wir die einzelnen Hardwareplattformen vor und bewerten diese, bevor wir das Kapitel mit einer Zusammenfassung abschließen.

3.1 Übersicht

Zunächst sind zwei grundlegende Kategorien der Hardwareplattformen zu unterscheiden.

- **Atomistische Plattformen** nutzen elementare Quantensysteme wie einzelne Atome, Ionen oder Photonen als Qubits. Isoliert betrachtet besitzen die elementaren Quantensysteme schon alle Eigenschaften für gute Qubits. Die Herausforderung besteht hier in der Kontrolle und Skalierbarkeit.

- **Festkörper Plattformen** basieren auf integrierten Schaltkreisen und sind daher gut kontrollierbar und skalierbar. Hier besteht die Herausforderung im Bau geeigneter elementarer Systeme, die als Qubit fungieren können.

3.2 Leistungsindikatoren

Die Leistungsindikatoren für Quantencomputerhardware der BSI-Studie basieren auf den sogenannten *DiVincenzo*-Kriterien [DI00]:

- **Qubits**: Skalierbare und gut charakterisierte Qubits existieren.
- **Initialisierung**: Die Möglichkeit, den Zustand der Qubits zu Beginn der Berechnung zu setzen, besteht.
- **Lange Dekohärenzzeit**: Die Dekohärenzzeit sollte viel länger sein als die Zeit für eine Gatteroperation.
- **Universelle Gatter**: Die zur Verfügung stehenden Gatter sollten in Kombination alle möglichen Operationen implementieren können.
- **Messung**: Die Möglichkeit, den Zustand jedes Qubits nach der Berechnung zu messen, ist vorhanden.

Obwohl diese Kriterien an sich wichtig sind, ist es (insbesondere in Hinblick auf mögliche Anwendungen) notwendig, die DiVincenzo-Kriterien weiter auszuführen und zu ergänzen. Dazu möchten wir hier noch folgende Leistungsindikatoren nennen:

- **Konnektivität und Gatter**: In echten Hardwaresystemen ist es selten möglich, jedes Qubit mit jedem anderen Qubit interagieren zu lassen. Zudem kann die Art der Gatter beschränkt sein. Es ist zwar möglich, universelle Operationen auch bei geringer Konnektivität und eingeschränkter Gatterauswahl zu implementieren, dadurch steigen jedoch die Kosten (Anzahl der Gatteroperationen), was aufgrund der endlichen Dekohärenzzeit ein Problem sein kann. Generell sind Systeme mit einer großen Konnektivität und Gatterauswahl zu bevorzugen.
- **Parallele Ausführung**: Insbesondere aufgrund der endlichen Dekohärenzzeit ist es notwendig, einen gegebenen Algorithmus in der kürzestmöglichen Zeit auszuführen. Falls zwei Operationen z.B. auf verschiedenen Qubits ausgeführt werden und sich darüber hinaus nicht beeinflussen, sollten sie parallel ausgeführt werden. Ein Quantencomputer, der parallele Operationen ermöglicht, ist also zu bevorzugen.
- **Frische Qubits**: Die Bereitstellung neu initialisierter Qubits in einem definierten Zustand auch während des Algorithmus ist insbesondere für Quantenfehlerkorrektur

wichtig. Daher sind Maschinen, die dies ermöglichen, zu bevorzugen.

Die genannten Leistungsindikatoren vermitteln ein vereinfachtes Bild der tatsächlichen Situation (vgl. [Wil+20]). Trotzdem kann es von Nutzen sein, mehrere Leistungsindikatoren auf eine einzelne Zahl abzubilden, um eine sehr grobe, aber einfache Einschätzung der Leistung eines Systems vorzunehmen. Ein bekanntes Beispiel für einen solchen vereinfachten Leistungsindikator ist das **Quantenvolumen** [Mol+18]. Es bezieht folgende Leistungsindikatoren mit ein:

- die Anzahl der physikalischen Qubits N,
- die Konnektivität,
- die Anzahl der ausführbaren Gatter, bevor die Dekohärenz die Informationen zerstört,
- den zur Verfügung stehenden Gattersatz und
- die Anzahl der Operationen, die parallel ausgeführt werden können.

Je größer das Quantenvolumen ist, desto performanter ist der Quantencomputer.

3.2.1 Klassifizierung des Entwicklungsstandes von Hardwareplattformen anhand der Skala der BSI-Studie

Die Autoren der BSI-Studie führen eine Skala zur Bewertung der verschiedenen Hardwareplattformen bezüglich ihrer Nutzbarkeit als vollständig fehlerkorrigierte Quantencomputer ein. Mit dieser Skala lassen sich auch NISQ-Maschinen sinnvoll bewerten, denn auch hier ist gute Fehlerkorrektur wichtig für eine gute Performanz. Die Skala lautet wie folgt:

- **Stufe A: Grundlegende Funktionalität** Hier wurden mindestens zwei Qubits in einem Experiment initialisiert, eine Gatteroperation durchgeführt und das Ergebnis ausgelesen. Dabei muss ein gewisses Maß an Kohärenz nachgewiesen worden sein.
- **Stufe B: Qualität der Operationen** Es wurden die Fehlerraten der Gatter gemessen, und alle Voraussetzungen für Quantenfehlerkorrektur sind gegeben.
- **Stufe C: Fehlerkorrektur** Quantenfehlerkorrektur wurde nachgewiesen. Die Fehlerrate der logischen Qubits ist kleiner als die der physikalischen Qubits.

- **Stufe D: Fehlertolerante Operationen** Vollständig fehlerkorrigierte und universelle Quantenoperationen auf logischen Qubits wurden demonstriert.

- **Stufe E: Algorithmen** Komplexe Algorithmen wurden auf fehlerkorrigierten logischen Qubits demonstriert.

Für NISQ-Anwendungen ist mindestens Stufe B notwendig. Mit jeder Stufe steigt jedoch die Wahrscheinlichkeit, einen Quantenvorteil zur erhalten.

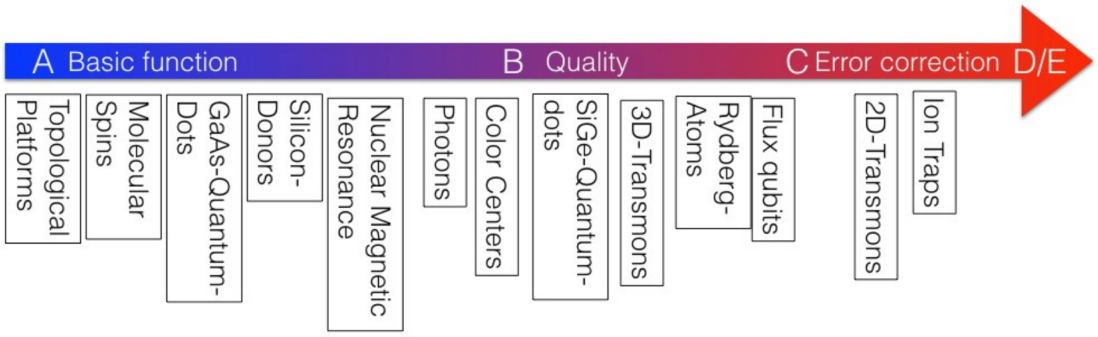

Abbildung 3.1: **Entwicklungsstufen und Einordnung der Hardwareplattformen nach der BSI-Studie [Wil+20]**

3.3 Evaluierung

In diesem Abschnitt folgen wir den Ausführungen der BSI-Studie [Wil+20], indem wir die verschieden Hardwareplattformen vorstellen und den o.g. Entwicklungsstufen zuordnen.[1]

3.3.1 Ionenfallen

Ionenfallen sind eine atomistische Plattform. Dadurch ist eine sehr gute Kontrolle und Isolation möglich. Sie bestehen aus ionisierten und damit geladenen Atomen, welche durch

[1] Einige Formulierungen in diesem Abschnitt sind nahezu direkte Übersetzungen aus der BSI-Studie [Wil+20]. Zugunsten der besseren Lesbarkeit verzichten wir jedoch auf Zitate in englischer Sprache.

elektromagnetische Felder räumlich fixiert werden. Die Qubits werden durch einzelne Elektronen in den äußeren Schalen der Atome realisiert und durch Laser oder Mikrowellenpulse manipuliert. Üblicherweise werden die Ionen in einer eindimensionalen Kette angeordnet und die Wechselwirkung erfolgt durch Vibrationsmoden. Ähnlich einer Reihe aus mit Federn verbundenen Perlen ist so eine Wechselwirkung aller Qubits untereinander prinzipiell möglich. Daher ist die Konnektivität in Ionenfallen vergleichsweise größer als z.B. in auf supraleitenden Schaltkreisen basieren Plattformen. Die große Herausforderung besteht jedoch in der Skalierbarkeit, welche zum Beispiel durch zweidimensionale Anordnung der Ionen realisiert werden könnte. Trotz großer Fortschritte wurde die Qualität von eindimensionalen Systemen noch nicht erreicht. Da grundlegende Quantencomputerprozesse mit hoher Qualität sowie einfache Quantenfehlerkorrektur demonstriert wurden, ordnen die Autoren der BSi-Studie [Wil+20] Ionenfallen in die Stufe C ein.

3.3.2 Supraleitende Schaltkreise

Supraleitende Schaltkreise sind die zur Zeit aussichtsreiche Technologie unter den Festkörperplattformen. Aufgrund der Notwendigkeit von Supraleitung müssen sie bei sehr tiefen Temperaturen betrieben werden, welches eine Komplikation aber keine grundsätzliches Hindernis darstellt. Eine der größten Herausforderung beim Bau und Betrieb von supraleitenden Qubits ist die Aufrechterhaltung von Kohärenz zur Fehlervermeidung. Die Kontrolle der Qubits geschieht üblicherweise über Mikrowellenpulse, welche neben der Kühlung räumlich an die supraleitenden Qubits herangeführt werden müssen. Wir gehen hier auf zwei verschiedene Varianten ein, Flussqubits und Transmonqubits.

Flussqubits sind supraleitende Schleifen, bei denen der Zustand des Qubits durch die Drehrichtung des Stroms durch die Schleife festgelegt ist. Durch den Kreisstrom wird ein magnetischer Fluss durch die Ebene der Schleife induziert, daher der Name Flussqubit. Zum Teil ist die Technologie ausgereift genug, um lange Kohärenzzeiten und einfache Kopplung zwischen den Qubits umzusetzen. Die Herausforderung besteht in der konsistenten Herstellung von Qubits mit vorhersagbaren Eigenschaften. Die Umsetzung des Gattermodells ist daher noch mit Hindernissen verbunden, insbesondere in Hinblick auf die Qualität von Mehr-Qubitgattern. Die BSI-Studie [Wil+20] ordnet Flussqubits daher in in Stufe B ein. Für Quantenannealer sind Flussqubits aufgrund der relativ hohen Konnektivität attraktiver. Sie werden daher von der Firma D-Wave Systems in deren Quantenannealern eingesetzt.

Eine alternative Implementierung von Qubits in supraleitenden Schaltkreisen sind Transmonen. Hier tragen Ladungsoszillationen in den supraleitenden Schaltkreisen die Quanteninformationen. Transmonqubits haben eine lange Kohärenzzeit und lassen sich einfach mit Hilfe von Mikrowellenresonatoren koppeln. Üblicherweise werden in zweidimensiona-

len Systemen die Kontroll- und Ausleseelektronik über die dritte Dimension zugeführt. Hier wurden Systeme mit geringer Konnektivität und einfache Quantenfehlerkorrektur demonstriert. Sie sind daher in Stufe C einzuordnen [Wil+20]. Dreidimensionale Transmonqubits besitzen tendenziell eine bessere Kohärenzzeit, da sich der Resonator hier auch in die dritte Dimension erstreckt. Allerdings ist es hier schwieriger, Kontroll- und Ausleseelektronik anzubinden. Daher werden dreidimensionale Transmonqubitsysteme in Stufe B eingeordnet.

3.3.3 Neutrale Atome

Wie bei Ionenfallen wird hier die Quanteninformation in den elektronischen Zuständen der Atome gespeichert. Wir beschränken uns hier auf Atome in Rydberg-Zuständen (auch Rydbergatome genannt) als den aussichtsreichen Kandidaten für Quantencomputer mit neutralen Atomen. Als Rydberg-Zustand wird der Zustand eines Atoms bezeichnet, bei dem das äußerste Elektron viel weiter von Kern entfernt ist als im Grundzustand. Dadurch besitzen Rydbergatome ein relativ großes Dipolmoment. Die langreichweitige Wechselwirkung zwischen den Dipolmomenten zweier Rydbergatome kann zur Realisierung von Gattern verwendet werden.

Eine der größten Herausforderungen bei Rydbergatomen ist es, die Atome räumlich zu fixieren. Aufgrund der elektrostatischen Neutralität ist dies nur mit Laser-induzierter dipolaren Wechselwirkung möglich. Diese ist jedoch viel kleiner als die elektromagnetischen Kräfte in Ionenfallen, und zusätzliche Laserkühlung ist nötig. Daher werden Rydbergatome zwischen Stufe B und Stufe C eingeordnet. Systeme mit Rydbergatomen spielen eine ungleich größere Rolle für Quantentechnologien jenseits des Computings, wie Quantenmetrologie und Simulation von Quantensystemen in Gittern.

3.3.4 Halbleiter

Klassische Halbleitertechnologie ist eine extrem ausgereifte Technologie. Ein Quantencomputer, der auf Halbleitertechnologie beruht, kann auf diese Errungenschaften zurückgreifen und stellt daher einen aussichtsreichen Kandidaten dar. Unter einer Vielzahl von Varianten begrenzen wir uns hier auf die mit dem größten Potenzial.

Dies sind zunächst einmal sogenannte Quantenpunkte. Das sind Halbleiterstrukturen, welche einzelne Elektronen fixieren und ähnliche Eigenschaften aufweisen wie ein *künstliches*

Atom. Die größte Herausforderung hier ist die Reduzierung von ladungsinduzierten Störungen zur Verbesserung der Kohärenz der Qubits. Die Anbindung von Steuerungs- und Ausleseelektronik hat viele Übereinstimmungen mit supraleitenden Plattformen und funktioniert vergleichsweise gut. Quantenpunkte werden daher in Stufe B eingeordnet.

Neben den Quantenpunkten gibt es noch Fehlstellen in Diamanten, die aus Fremdatomen bestehen. Diese funktionieren ähnlich wie Ionenfallen, nur das sie durch die Gitterstruktur des Diamanten fixiert werden. Fehlstellen in Diamanten spielen hauptsächlich in der Quantensensorik und Quantenphotonik eine Rolle. Die größte Herausforderung besteht hier in der konsistenten Bereitstellung der Qubits, weshalb die Ansteuerung noch über optische Netzwerke erfolgen muss. Diese verhindern zur Zeit eine großskalige Umsetzung. Die Technologie wird daher in Stufe A eingeordnet. Es ist jedoch zu bemerken, dass die BSI-Studie im Falle der Lösung des Bereitstellungsproblems ein rasches Aufholen der Technologie bis zu Stufe C erwartet [Wil+20].

Zuletzt möchten wir hier noch topologische Qubits erwähnen. Obwohl diese auf verschiedenen Plattformen verfolgt werden, erscheinen eindimensionale nanoskopische Halbleiterstrukturen als aussichtsreichste Kandidaten. Bei topologischen Qubits werden die Quanteninformationen in Vielteilchenanregungen (welche auch als Quasiteilchen bezeichnet werden) gespeichert. Die Besonderheit besteht darin, dass diese Anregungen bereits auf der Ebene des Materials *topologisch* gegen Fehler geschützt sind. Nur sehr unwahrscheinliche andere Vielteilchenanregungen können die Qubits stören. Da selbst einzelne topologische Qubits nicht zweifelsfrei demonstriert werden konnten, befindet sich die Technologie in Stufe A. Ein Durchbruch brächte sie jedoch aufgrund der eben genannten Vorteile schnell in Stufe D [Wil+20].

3.3.5 Photonen

Bei photonischen Plattformen werden die Quantenteilchen des Lichts, die Photonen, als Träger der Informationen genutzt. Eine Schwierigkeit besteht in der Implementierung von Zwei-Qubitgattern. Da Photonen nicht direkt wechselwirken, müssen indirekte Wechselwirkungen genutzt werden. Bis jetzt reicht die Gatterqualität nicht zur Anwendung von Quantenfehlerkorrektur aus. Aufgrund der hohen Lichtgeschwindigkeit ist es zudem unklar, wie ein großskaliges System auf kleinem Raum umgesetzt werden kann. Daher wird die Technologie in Stufe B eingeordnet [Wil+20].

3.4 Zusammenfassung

Heutzutage ist es unmöglich, einen klaren Favoriten für eine Quantencomputerplattform zu identifizieren. Ionenfallen und einige supraleitende Schaltkreise (2D-Transmonen) sind zur Zeit am weitesten fortgeschritten (Stufe C). Dahinter folgen Rydbergatome, andere supraleitende Schaltkreise (Flussqubits, 3D-Transmonen) und Halbleiter (Stufe B) sowie etwas niedriger Photonen. Topologischen Qubits sowie gewissen Halbleiterqubits wird bei technologischen Durchbrüchen ein rasches Aufholen zugetraut.

4 Algorithmen, Software und Anwendungen

In diesem Kapitel geben wir einen Überblick über Algorithmen für Quantencomputer und deren Anwendung. Der erste Teil behandelt die wichtigsten Algorithmen unterteilt nach der Hardware, auf denen sie ausgeführt werden können. Anschließend behandeln wir Software zur Steuerung von Quantencomputern sowie zur Implementierung von Quantenalgorithmen zur Lösung relevanter Probleme. Im letzten Teil des Kapitels werden die möglichen Anwendungen für zuvor diskutierte Quantenalgorithmen vorgestellt, bevor wir mit einer Zusammenfassung abschließen.

4.1 Algorithmen

4.1.1 Algorithmen für fehlerkorrigierte Quantencomputer

Hier behandeln wir Algorithmen, welche vollständige Quantenfehlerkorrektur benötigen. Wie bereits im Kapitel 2 beschrieben, werden hier mehrere physikalische Qubits zusammengefasst, um dem Programmierer vollständig fehlerfreie logische Qubits zur Verfügung zu stellen. Im Allgemeinen zeichnen sich diese Algorithmen einerseits dadurch aus, dass deren Performanz in Abhängigkeit der Problemgröße bekannt ist. Andererseits ist ihre Umsetzung weiter entfernt als die von Algorithmen, die mit fehlerbehafteten Quantencomputern zurecht kommen.

Der wohl bekannteste Quantenalgorithmus ist der **Shor-Algorithmus** [Sho94] zur Faktorisierung großer Zahlen. Der Algorithmus besteht aus einem klassischen Teil und einem Teil, der auf dem Quantencomputer ausgeführt wird. Letzterer beruht auf der **Quanten-Fouriertransformation**, welche eine häufige Unterroutine in Quantenalgorithmen ist. Der gesamte Algorithmus erhält als Eingabe eine zu faktorisierende Zahl der Größe n und gibt nach einer Laufzeit der Größenordnungen $\mathcal{O}((\log n)^3)$ einen nicht-trivialen Faktor von

n aus. Da die Laufzeit des besten bekannten rein klassischen Algorithmus exponentiell mit der Problemgröße wächst, stellt der Shor-Algorithmus eine exponentielle Laufzeitverbesserung dar.

Ein weiterer bekannter Quantenalgorithmus ist der **Grover-Algorithmus** [Gro96]. Dieser Algorithmus findet mit hoher Wahrscheinlichkeit die Eingabe einer unbekannten Funktion bei Kenntnis des Ausgabewertes. Hierbei werden nur $\mathcal{O}(\sqrt(n))$ Auswertungen der Funktion benötigt, wobei n die Anzahl der unterschiedlichen Eingabewerte der Funktion ist. Der beste klassische Algorithmus benötigt $\mathcal{O}(n)$ Auswertungen der Funktion, wodurch sich eine polynomielle Laufzeitverbesserung ergibt. Analog kann man sich den Algorithmus auch als Suchalgorithmus in einer Datenbank vorstellen. Diese Datenbank besteht dann aus einer Tabelle mit den Funktionswerten und den Indizes der Eingabewerte. Es ist zu beachten, dass für die Implementierung des Grover-Algorithmus eine Funktion auf dem Quantencomputer ausgewertet werden muss, die entscheidet, ob die Eingabe das gesuchte Ergebnis ist. Diese Funktion muss also effizient ausführbar sein, um den polynomiellen Quantenvorteil nicht wieder zunichtezumachen.

Des Weiteren gibt es den sogenannten **HHL-Algorithmus** [HHL09], benannt nach seinen Autoren Harrow, Hassidim und Lloyd. Dieser Algorithmus löst lineare Gleichungssysteme exponentiell schneller als der beste klassische Algorithmus. Allerdings müssen dafür eine Reihe von Bedingung erfüllt sein, die einer Anwendung noch im Wege stehen. Eine der wichtigsten Einschränkungen betrifft das sogenannte **Ein- und Ausgabeproblem**: Sowohl die Eingabedaten (also das Gleichungssystem) als auch die Ausgabe (die Lösung des Gleichungssystems) sind in den Amplituden eines Quantenregisters gespeichert. Eine effiziente Methode zum Ein- und Auslesen zwischen klassischem Speicher und einem Quantenregister ist bisher nicht bekannt. Darüber hinaus muss das lineare Gleichungssystem gut konditioniert sein, was die möglichen Anwendungsszenarien weiter einschränkt.

Neben den bereits genannten, bekanntesten Quantenalgorithmen gibt es eine Vielzahl von weniger bekannten Algorithmen. Der Grund für die niedrigere Bekanntheit spiegelt nicht unbedingt das Potenzial dieser Algorithmen wieder und ist vielmehr der Komplexität der Algorithmen und insbesondere der vielen Einschränkungen, unter denen sie einen Quantenvorteil garantieren, geschuldet. Eine Beispiel für einen solchen Algorithmus ist ein Algorithmus zum Mustererkennung [HV03; Mon17] mit superpolynomiellem Quantenvorteil. Weitere Beispiele finden sich im *Quantum Algorithm Zoo* [Qua].

4.1.2 Algorithmen für fehlerbehaftete Quantencomputer (NISQ)

Im Gegensatz zu herkömmlichen Quantenalgorithmen, wie sie im Abschnitt 4.1.1 beschrieben sind, kommen Algorithmen für fehlerbehaftete Quantencomputer (NISQ) üblicherweise ohne Quantenfehlerkorrektur aus. Dabei handelt es sich jedoch größtenteils um Heuristiken, weshalb eine allgemeine Aussage über die Laufzeit in Abhängigkeit der Problemparameter nicht möglich ist. Trotzdem gibt es für solche Algorithmen Hinweise auf eine Laufzeitverbesserung. Zudem wird davon ausgegangen, dass die Forschung an NISQ-Algorithmen mit zunehmender Verbesserung der Hardware Fehlerkorrekturmechanismen mit einschließen wird.

Die hier vorgestellten Algorithmen sind allesamt **variationelle Quantenalgorithmen**. Bei diesen handelt es sich um sogenannte **hybride Algorithmen** bei denen klassische Computer und Quantencomputer zusammenarbeiten. Die Funktionsweise variationeller Quantenalgorithmen ist in Abbildung 4.1 dargestellt. In einem solchen Algorithmus wird auf ein Quantenregister ein Schaltkreis angewendet, welcher von einer Reihe klassischer Parameter $\boldsymbol{\theta} = (\theta_0, \ldots, \theta_N)$ abhängt. Dadurch entsteht ein Quantenzustand, der ebenfalls von diesen Parametern abhängt. Gesucht ist nun ein Satz von Parametern und der dazugehörige Quantenzustand, welcher eine gewisse Funktion $F(\boldsymbol{\theta})$ minimiert. Diese Funktion kann durch wiederholte Messung des Registers nach Anwendung des parametrisierten Schaltkreises angenähert werden. Um geeignete klassische Parameter zu finden und damit die Funktion zu minimieren, wird ein klassischer Optimierungsalgorithmus verwendet. Dieser beginnt mit einem Anfangssatz von Parametern und gibt diese an den Quantencomputer. Letzterer wertet die Funktion aus und gibt den Funktionswert an den klassischen Computer zurück. Dieser schlägt daraufhin neue Parameter vor. Die Prozedur wird solange wiederholt, bis die Zielfunktion minimiert ist. Eine Variante solcher variationeller Algorithmen berechnet neben der Zielfunktion auch den Gradienten der Zielfunktion auf dem Quantencomputer.

Wir beschränken uns hier auf drei Beispiele variationeller Quantenalgorithmen. Zunächst gibt es den *Quantum Approximate Optimization Algorithm* (**QAOA**) [FGG14]. Ziel dieses Algorithmus ist die Lösung kombinatorischer Optimierungsprobleme, welche sich als pseudo-Boolsche Funktionen darstellen lassen (vgl. Abschnitt 2.3). Dabei führt der Schaltkreis alternierend zwei parametriesierte Operationen durch: Die erste Operation enthält die zu optimierende Funktion und treibt das Quantenregister in Richtung lokaler Minima. Im Gegensatz dazu stellt die zweite Operation Überlagerungen von Lösungen her. Diese Operation wird auch *Mixer* genannt. Sie hilft damit lokale Minima zu überwinden und dem globalen Minimum näher zu kommen.

Als zweites Beispiel möchten wir **Quanten-Neuronale-Netze (QNN)** [Bia+17] diskutie-

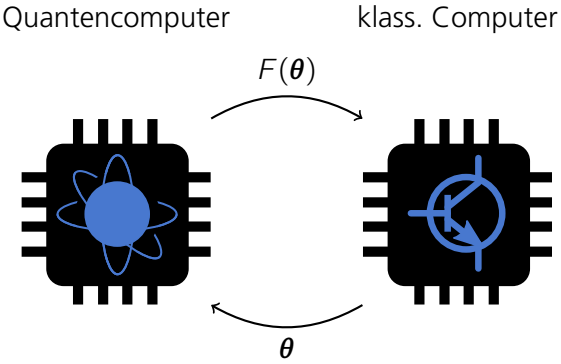

Abbildung 4.1: **Funktionsweise variationeller Quantenalgorithmen: Der Quantencomputer liefert die Funktionsauswertung $F(\boldsymbol{\theta})$ und der klassische Computer liefert den nächsten zu überprüfenden Parametersatz $\boldsymbol{\theta}$.**

ren. Klassische neuronale Netze bestehen aus einem Netz von künstlichen Neuronen. Diese künstlichen Neuronen sind parametrisierte Funktionen, welche Eingänge und Ausgänge haben. Die Parameter werden in Bezug auf eine Zielfunktion (welche von den zu lernenden Daten abhängt) optimiert. Diesen Vorgang bezeichnet man dann als maschinelles Lernen. In einem QNN werden die künstlichen Neuronen durch parametrisierte Quantengatter ersetzt. Dadurch erhofft man sich überlegene Eigenschaften durch Superposition und Verschränkung, welche durch klassische Computer (inklusive künstlicher Neuronen) nicht abgebildet werden können.

Das letzte und vielleicht vielversprechendste Beispiel sind **variationelle Quanten-Eigenlöser (VQE)** [Mol+18]. Bei diesem Algorithmus wird versucht, mit Hilfe eines Quantencomputers den niedrigsten Energiezustand eines Quantensystems zu simulieren. Der parametrisierte Schaltkreis orientiert sich hier an klassischen Ansätzen, z.B. aus der Quantenchemie, und die Kostenfunktion ist die Energie des zu simulierenden Systems. Die Hauptanwendung ist somit Quantensimulation für Festkörpersysteme oder Moleküle. Insbesondere für Quantensysteme mit starken Korrelationen steigt der Rechenaufwand bei klassischen Verfahren exponentiell mit der Problemgröße an. Es besteht die Hoffnung, dass VQE-Algorithmen hier eine extreme Laufzeitverbesserung liefern könnten.

4.1.3 Berechnungen mit Quantenannealern

Wie schon in Kapitel 2 erwähnt, berechnen Quantenannealer tiefliegende Zustände pseudo-Boolscher Funktionen. Im Prinzip ähneln sie damit sehr dem QAOA-Algorithmus aus dem

vorhergehenden Kapitel. Obwohl Quantenannealer sich nicht analog zu gatterbasierten Quantencomputern programmieren lassen, gibt es doch eine Reihe von Einstellmöglichkeiten, die einem *analogen Algorithmus* ähneln. Dies sind insbesondere die Kraftfelder, die auf das System zu Beginn der Berechnung wirken. Der zugehörige Quantenoperator wird üblicherweise als *Driver* bezeichnet. Dies ist ähnlich zum *Mixer* im QAOA-Algorithmus. Analog wird der Quantenoperator, der der pseudo-Boolschen Funktion entspricht, als *Problem-Hamilton-Operator* bezeichnet. In einem D-Wave Quantenannealer entspricht der Driver einem transversalen magnetischen Feld, falls man alle Qubits als elementare magnetische Momente auffasst (Spins). Im Prinzip ist die Wahl des Drivers jedoch offen und hat einen extremen Einfluss auf die Erfolgswahrscheinlichkeit der Berechnung [NT17]. Die Berechnung im Quantenannealer erfolgt durch langsames Zurückfahren des Drivers und gleichzeitiges Hochfahren des Problem-Hamilton-Operators. Wie genau die Mischung der beiden Operatoren über den Zeitraum der Berechnung erfolgt, kann jedoch variiert werden. Dieser *Fahrplan* hat auch einen großen Einfluss auf die Performanz des Ansatzes [ONL18].

4.2 Software

Um eine Anwendungsproblem auf einem Quantencomputer zu lösen, müssen eine Vielzahl von Schritten in Form von Softwareabstraktionsschichten ausgeführt werden. Diese Schritte werden wir hier in vier Kategorien einteilen. Siehe Abbildung 4.2. Zunächst gibt es die **Anwendungsschicht**. Hier werden die klassischen Daten eingelesen, konfektioniert und vorprozessiert. Dabei gilt es nur solche Rechenoperationen für den Quantencomputer vorzusehen, bei denen eine Laufzeitverbesserung zu erwarten ist. Der Quantencomputer ist hierbei ein Koprozessor, der Teilprobleme löst, ähnlich wie Grafikprozessoren in heutigen Computersystemen, jedoch mit völlig anderen Eigenschaften. Der nächste Schritt ist die Übergabe des Teilproblems an einen geeigneten **Quantenalgorithmus**. Die Operationen in solchen Quantenalgorithmen sind selten direkt auf der Hardware ausführbar. Dazu ist ein **Kompilierungsschritt** notwendig. Dieser umfasst insbesondere die Abbildung der gewünschten Gatteroperationen auf die tatsächlich möglichen Gatteroperationen, die Optimierung der Schaltkreise zur Verbesserung der Laufzeit und Maßnahmen zur Quantenfehlerkorrektur. Letztere werden auf NISQ-Maschinen noch keine große Rolle spielen, mit den Fortschritten in der Hardwareentwicklung jedoch immer mehr in den Fokus rücken. Die letzte Softwareschicht umfasst die **Kontrolle der Hardware**. Hier geht es darum, die gewünschten Gatteroperationen tatsächlich in der Hardware umzusetzen und Ergebnisse auszulesen. Dabei gilt es, die Fehler möglichst gering zu halten und idealerweise die Charakteristika der Fehler an die Kompilierungsschicht zurückzumelden.

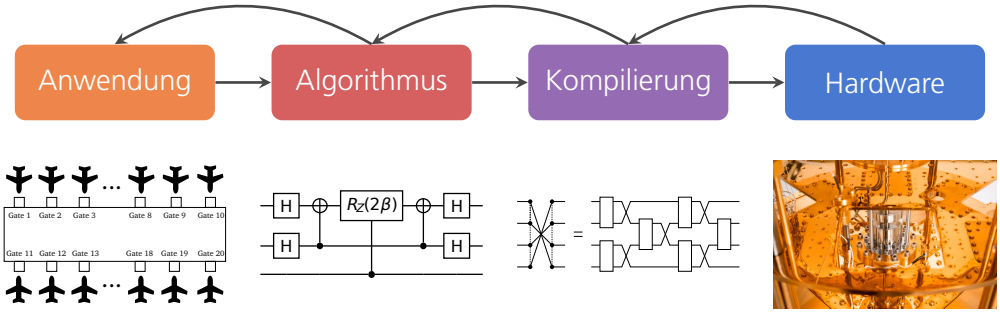

Abbildung 4.2: **Softwareabstraktionsschichten im Paradigma des Hardware-Software-Codesign.**[1]

Diese Abstraktionsschichten sind jedoch keinesfalls unabhängig voneinander. Aufgrund des frühen Stadiums der Entwicklung von Quantencomputern und Quantenalgorithmen finden regelmäßig disruptive Änderungen statt. Daher ist die Entwicklung von standardisierten Schnittstellen und automatischen Abbildungs- und Kompilierungsschichten, welche für eine Vielzahl von Anwendungen und Hardwareplattformen gültig sind, keinesfalls sinnvoll oder zielführend. Vielmehr müssen die Softwareschichten auf allen Ebenen, von der Anwendung bis zur Kontrolle der Hardware, ineinandergreifen. Dieses Paradigma wird als **Hardware-Software-Codesign** bezeichnet und setzt eine intensive Zusammenarbeit von Anwender(inne)n, Algorithmiker(inne)n und Hardwareentwickler(inne)n voraus. Nur so wird es möglich sein, einen Quantenvorteil für eine sinnvolle Anwendung zu demonstrieren. Natürlich haben solche Lösungen ein Stück weit einen prototypischen Charakter. Aber sie werden als Ausgangspunkt für generische Lösungen dienen. Man beachte, dass die heutigen Compiler für klassische Hardware eine jahrzehntelange Entwicklung hinter sich haben. Auch hier waren lange Zeit disruptive Veränderungen der Hardware die Regel, bevor sich einige wenige Plattformen und die dazugehörigen Schnittstellen durchsetzten. Nichtsdestotrotz werden auch für heutige, klassische High-Performance-Systeme Algorithmen und Software zielgenau auf die Hardware angepasst, um eine maximale Performanz zu erreichen. Auf absehbare Zeit wird ein Quantencomputer daher nur mit Hilfe von Experten und Expertinnen sinnvoll programmiert werden können.

[1] Photo: OpenSuperQ, Forschungszentrum Jülich, Ralf-Uwe Limbach

4.3 Anwendungen

In diesem Abschnitt stellen wir die wichtigsten möglichen Anwendungen für Quantencomputeralgorithmen vor. Die Reihenfolge ist dabei nicht zufällig, sie folgt vielmehr lose einem Trend von noch weit entfernten Anwendungen (Kryptographie) zu Anwendungen, die vermutlich in näherer Zukunft einsetzbar sind (Quantensimulation).

4.3.1 Kryptoanalyse und Kryptographie

Eine Anwendung, die immer wieder mit Quantencomputern in Verbindung gebracht wird, ist die **Kryptoanalyse**, also das entschlüsseln verschlüsselter Informationen. Insbesondere asymmetrische Kryptographieverfahren beruhen auf der Annahme, dass große Zahlen sich nicht effizient faktorisieren lassen. Genau hier setzt der Shor-Algorithmus [Sho94] an, welcher, wie oben beschrieben, große Zahlen effizient faktorisieren kann. Aufgrund der Notwendigkeit von Quantenfehlerkorrektur und der damit verbundenen großen Zahl von Qubits sind für realistische Fehlerraten mehrere Millionen Qubits erforderlich, um ein gängiges Verfahren wie RSA-2048 zu brechen [Wil+20]. Ein solches Anwendungsszenario ist daher höchstens langfristig denkbar. Umgekehrt ist jedoch wichtig, klassische Kryptographie gegen zukünftige Angriffe mit Quantencomputern abzusichern.

Im Gegensatz zur Kryptoanalyse spielen Quantencomputer in der Kryptographie, also der Verschlüsselung von Informationen, nur indirekt eine Rolle. Es gibt zwar teilweise Überschneidungen zwischen Quantenkryptographie und Quantencomputing, diese gehen jedoch nicht über die Tatsache hinaus, dass in beiden Disziplinen Quanteninformationen verarbeitet werden. Insbesondere kann ein Quantencomputer, wie er in dieser Studie beschrieben wird, nicht direkt für Quantenkryptographie eingesetzt werden.

4.3.2 Simulation klassischer Systeme

Die Simulation von klassischen Systemen wie Strömungen oder elektromagnetischer Strahlung hat zahllose Anwendungen, insbesondere in den Ingenieurwissenschaften. Eine großes Anwendungsfeld hat die numerische Lösung **partieller Differentialgleichungen**, deren Diskretisierung meist zur Lösung großer **linearer Gleichungssysteme** führt. Da der im Abschnitt 4.1.1 beschriebene HHL-Algorithmus lineare Gleichungssysteme unter Umständen exponentiell schneller lösen kann als die besten klassischen Verfahren, erscheint die

Anwendung von Quantencomputern für diese Anwendung zunächst attraktiv. Die Einschränkungen des Algorithmus verengen die möglichen Anwendungsbereiche jedoch extrem. Trotzdem gibt es mögliche Anwendungen des HHL-Algorithmus, wie zum Beispiel die Radarquerschnittsberechnung [CJS13], bei der das Ein- und Ausgabeproblem teilweise nicht auftritt. Trotzdem ergeben Abschätzungen für die benötigten Quantenressourcen Millionen von Qubits und Gattern [CJS13; Zac19], was die Anwendung in weiter Ferne rückt.

Neben diesen Ansätzen für vollständig fehlerkorrigierte Quantencomputer, gibt es seit Kurzem auch variationelle Ansätze zur Lösung von **partiellen Differentialgleichungen** [Lub+20], welche eher für NISQ-Maschinen geeignet sind. Wie für alle variationellen Ansätze auf NISQ-Maschinen ist eine Abschätzung der Performanz jedoch schwierig, und zudem gibt es noch erhebliche Einschränkungen, was die Breite der Anwendungen angeht.

4.3.3 Maschinelles Lernen

Unter dem Begriff *quanten-maschinelles Lernen* (QML) werden verschiedene Disziplinen zusammengefasst, welche wir zunächst differenzieren möchten. Es hat sich als nützlich erwiesen, sowohl die Art der Daten als auch den Algorithmus nach den Attributen *klassisch* und *quantenmechanisch* zu unterscheiden. Diese Unterscheidung ist in Abbildung 4.3 verdeutlicht. Das Lernen aus quantenmechanischen Daten (QK und QQ in Abbildung 4.3)

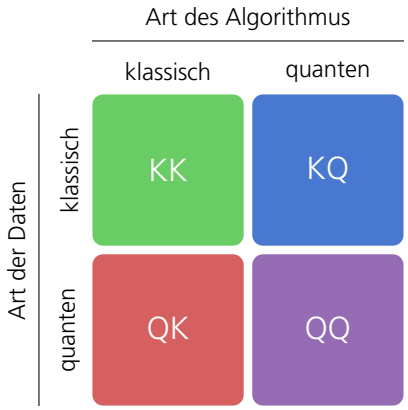

Abbildung 4.3: **Vier verschiedene Ansätze für quanten-maschinelles Lernen**

ist für experimentalphysikalische Quantensysteme relevant. Wir werden es nicht weiter behandeln. Gleiches gilt für das Lernen aus klassischen Daten mit klassischen Methoden (KK in Abbildung 4.3). Wir konzentrieren uns hier auf das Lernen aus klassischen Daten

mit quantenmechanischen Methoden (KQ in Abbildung 4.3), welches oft als *quantenbeschleunigtes maschinelles Lernen* bezeichnet wird.

Zum einen gibt es Ansätze, die auf dem HHL-Algorithmus aufbauen, wie eine Methode der kleinsten Quadrate für maschinelles Lernen [WBL12]. Diese leiden unter den gleichen, schon genannten, Einschränkung durch extensiven Ressourcenverbrauch und das ungelösten Ein- und Ausgabeproblem. Zum anderen gibt es eine Reihe von Heuristiken für quantenbeschleunigtes maschinelles Lernen [Bia+17]. Beispiele sind unter anderem quantenbeschleunigtes, verstärktes Lernen [Pap+14], Quanten-Boltzmann-Maschinen [Ami+18], oder Quanten-Neuronale-Netze [CCL19].

Da überwachtes und unüberwachtes maschinelles Lernen nur mit enormen Datenmengen erfolgreich sein kann, sind Verfahren, die eine große klassische Datenmenge im Quantenregister annehmen und damit das Ein- und Ausgabeproblem ignorieren, nicht besonders aussichtsreich. Leider wird dies in vielen Publikationen noch ignoriert, was den frühen Entwicklungsstand des Forschungsfeldes widerspiegelt. Zudem ist zur Zeit noch völlig unklar, ob Quantencomputer Verfahren des maschinellen Lernens überhaupt beschleunigen können.

4.3.4 Optimierung

Zunächst einmal ist zwischen kontinuierlichen und diskreten Optimierungsproblemen zu unterscheiden. Erstere haben eine große Relevanz, insbesondere für ingenieurwissenschaftliche Fragestellungen. Ihre Umsetzung auf Quantencomputern erscheint zur Zeit jedoch noch sehr schwierig, aber in Zusammenhang mit dem in Abschnitt 2.4 beschriebenem Quantencomputing mit kontinuierlichen Variablen denkbar.

Anders verhält es sich mit diskreten (kombinatorischen) Optimierungsproblemen. Solche Probleme sind üblicherweise schwer zu lösen, d.h. die Laufzeit wächst exponentiell mit der Problemgröße. Der Anwendungsbereich ist hierbei sehr breit und umfasst unter anderem Logistikprobleme, Planungsprobleme in der industriellen Herstellung, Operations Research, Verkehrsplanung und Netzwerkprobleme. Hier können kleine Verbesserungen in der Laufzeit oder Lösungsqualität eine enorme Ersparnis in Form von Kosten oder CO_2-Ausstoß bedeuten. Daher ist selbst mögliche polynomielle Laufzeitverbesserung mit Quantencomputern von höchster praktischer Relevanz.

Grovers Algorithmus lieferte eine garantierte, polynomielle Laufzeitverbesserung und kann im Prinzip auf kombinatorische Optimierungsprobleme angewendet werden. Aufgrund der

nötigen Quantenfehlerkorrektur ist die tatsächliche Performanz auf fehlerbehafteten Maschinen unklar. Ähnlich verhält es sich mit dem QAOA-Algorithmus und Quantenannealing, welche für NISQ-Maschinen konzipiert sind, aber aufgrund ihrer heuristischen Natur keine Laufzeitverbesserung garantieren. Hier ist die erfolgversprechendste Strategie zur Erreichung eines Quantenvorteils das experimentelle Testen und sukzessive Verbessern der Heuristiken an realistischen Probleminstanzen.

4.3.5 Quantensimulation

Die ursprüngliche Idee Richard Feynmans für einen Quantencomputer war es, ihn zur Simulation von Quantensystemen zu verwenden [Fey86]. Auch heutzutage erwarten die meisten Experten, dass diese Anwendung am geeignetsten ist, um einen Quantenvorteil zu demonstrieren. Insbesondere für stark korrelierte Quantensysteme, bei den Verschränkung eine große Rolle spielt, wächst der Rechenaufwand mit klassischen Computern exponentiell mit der Problemgröße, während für Quantencomputer eine polynomieller Rechenaufwand erwartet wird. Dies bedeutet also eine exponentielle Leistungsverbesserung. Solche stark korrelierten Systeme kommen unter anderem in der Molekülchemie oder der Festkörperphysik vor. Mögliche Endanwendungen sind z.B. Material- und Medikamentenentwicklung in der Chemie und Pharmaindustrie.

Bei der Simulation von Quantensystemen mit klassischen Computern kann auf eine jahrzehntelange Erfahrung zurückgegriffen werden. Es gibt hervorragende Methoden zur Simulation von schwach und stark korrelierten Systemen. Wie bereits erwähnt, wäre es erfolgversprechend, den stark korrelierten Teil mit einem Quantencomputer zu ersetzten und den unkorrelierten Teil weiterhin mit einem klassischen Computer auszuführen. Hier besteht jedoch erheblicher Entwicklungsbedarf, was Algorithmen und Software angeht: Es ist noch nicht klar, wie ein solcher, hybrider Algorithmus genau aussehen könnte und wie die Schnittstellen definiert werden.

Neben Quantencomputern können auch spezielle Quantensimulatoren für die Simulation verwendet werden. Mit Quantensimulatoren bezeichnen wir experimentelle Quantensysteme, mit denen sich andere Quantensysteme simulieren lassen. Der Übergang ist fließend, wobei ein Quantencomputer eine möglichst universelle Schnittstelle hat und reproduzierbare Ergebnisse liefert, wohingegen ein Quantensimulator eine speziell für einen eng gefassten Zweck gebaute Maschine ist.

4.4 Zusammenfassung

Die Entwicklung von Algorithmen und Software mit Hinblick auf aussichtsreiche Anwendungen voranzutreiben, ist neben der Hardwareentwicklung von essentieller Bedeutung. Aufgrund des frühen Stadiums der Hardwareentwicklung, und der damit zusammenhängend Volatilität, ist es notwendig, dass Software- und Hardwareentwickler eng zusammenarbeiten. Für eine Programmierung der Maschinen ohne tiefere Kenntnisse der Hardware oder gar standardisierte Softwareschnittstellen ist es noch zu früh. Die Simulation von Quantensystemen wird als aussichtsreicher Kandidat für die Demonstration eines Quantenvorteils gesehen. Dahinter folgen kombinatorische Optimierung und anschließend maschinelles Lernen. Numerische Verfahren, wie sie in der Simulation von klassischen Disziplinen wie Fluiddynamik oder Elektrodynamik vorkommen, erscheinen noch weiter entfernt. Gleiches gilt für kryptografische Anwendungen.

5 Nationale und internationale Akteure

In diesem Kapitel geben wir eine Übersicht über die wichtigsten Akteure aus Industrie und Forschung. Dabei liegt der Fokus auf Deutschland und verbündeten Nationen. Zunächst geben wir einen Überblick, bevor wir einzeln auf Akteure in der Hardware- und Softwareentwicklung sowie mögliche Endanwender eingehen. Des Weiteren behandeln wir das Marktpotenzial für Unternehmen im Bereich Quantencomputing. Zuletzt schildern wir unsere Sicht auf mögliche Aktivitäten des DLR in der Quantencomputerentwicklung.

5.1 Überblick

Die Haupttreiber der Entwicklung sind nordamerikanische Akteure. Eine große Menge Wagniskapital ist den letzten zwei Jahrzehnten in die Entwicklung von Quantencomputerhardware geflossen. Aber auch die Algorithmenforschung ist traditionell stark in den USA und Kanada. Dies führte dazu, dass sowohl Großunternehmen wie Google, IBM, Microsoft, Intel und Amazon als auch Start-ups wie D-Wave und Rigetti weltweit führend in der Entwicklung von Quantencomputern sind.

In Europa gibt es eine starke Grundlagenforschung, sowohl im Hardwarebereich als auch unter Algorithmenforschern. Im Gegensatz zu den USA gab es lange Zeit keine Investitionen und wenig Expertise, um die Quantencomputing-Theorie in der Praxis zu nutzten. Dies beinhaltet sowohl die Herstellung von Hardware im industriellen Umfeld als auch die praxisorientierte Entwicklung von Algorithmen. Die Brücke von der Grundlagenforschung zur Anwendung kann nur von Experten ausgehen, welche die Grundlagen verinnerlicht haben. Mit dem umgekehrten Weg, bei dem man Quantencomputer nur von der Anwendungsseite betrachtet und damit gewissermaßen als *Black Box* behandelt, wird es schwer, einen Quantenvorteil zu demonstrieren. Der Grund für die Zurückhaltung, sowohl auf Entscheiderseite als auch auf Expertenseite, ist einleuchtend: Für die Umsetzung von praktischem Quantencomputing sind große Investitionen, insbesondere für die Hardwareentwicklung,

notwendig. Gleichzeitig ist der mögliche Nutzen zwar unter Umständen extrem groß, aber keineswegs sicher.

Auch wenn die USA einen großen Vorsprung hat, spricht einiges dafür, Quantencomputing in Europa und Deutschland voranzutreiben. Die wichtigsten Gründe sind technologische Souveränität und Positionierung der Industrie in einem wichtigen Zukunftsmarkt. Dazu bedarf es allerdings konzentrierter und entschlossener Initiativen. Aufgrund des teilweisen Vorsprungs anderer europäischer Länder, wie dem Vereinigten Königreich, den Niederlanden, Österreich und der Schweiz, sollten die deutschen Initiativen idealerweise im europäischen Kontext erfolgen.

Wie in bereits in Abschnitt 4.2 erwähnt, ist es sinnvoll, Initiativen voranzutreiben, bei denen die Hardware- und Softwareentwicklung im engen Austausch stattfindet. Des Weiteren sollten sowohl Grundlagenforscher als auch mögliche Endanwender bei der praktischen Umsetzung von Quantencomputing beteiligt werden. Zur Zeit gibt es jedoch wenig Austausch zwischen diesen Gruppen. Die möglichen Endanwender drängen auf die Entwicklung von Anwendungssoftware und dem Zugang zu Quantencomputerhardware, auch wenn diese nur eingekauft wird. Das Verfolgen dieser Strategie alleine birgt jedoch die Gefahr, mittelfristig technologisch abgehängt zu werden. Vielmehr ist es notwendig, die Brückenbauer zwischen Grundlagenforschern und möglichen Endanwendern zu stärken, welche über die Expertise verfügen, mit beiden Gruppen zu interagieren. Dazu zählen in Europa unter anderem die europäischen Projekte wie OpenSuperQ, AQTION und NEASQC, Start-ups wie HQS, Cambridge Quantum Computing, IQM, Alpine Quantum Technologies, aber auch Forschungszentren wie das FZ Jülich (JUNIQ, Michielsen, Wilhelm-Mauch) oder (in kleinerem Umfang) die Quantencomputinggruppe des Autors im Institut für Softwaretechnologie des DLR.

Außerhalb Europas und Nordamerikas möchten wir hier noch andere Akteure erwähnen. Zunächst gibt es in China massive Investitionen in Quantencomputing, die erwarten lassen, dass die technologische Entwicklung weiter fortgeschritten ist als in Europa, jedoch nicht den US-amerikanischen Stand erreicht. Eine genaue Einschätzung ist jedoch schwierig. Gleiches gilt für Russland, welches über sehr gute Grundlagenforscher verfügt. Es wird jedoch angenommen, dass Russlands Entwicklung hinter der Europas zurücksteht. Japan und Australien haben einen ähnlichen Entwicklungsstand wie Europa, wobei Japan aufgrund der dort ansässigen großen Zahl von Elektronikherstellern unter Umständen einen Vorteil besitzt.

5.2 Hardware

In diesem Abschnitt beschreiben wir die wichtigsten nationalen und eine Auswahl internationaler Akteure im Bereich Hardwareentwicklung für Quantencomputer. Dies beinhaltet auch Forscher, die sich mit der für Quantencomputerhardware relevanten Theorie beschäftigen.

5.2.1 Industrie

Zurzeit sind nordamerikanische Firmen in der Quantencomputerhardwareentwicklung führend. **D-Wave** war die erste Firma, die kommerziell Quantencomputerhardware in Form von auf Flussqubits basierenden Quantenannealern auf dem Markt brachte. **Google**, **IBM**, **Rigetti** und **Intel** bauen gatterbasierte Quantencomputer auf Basis von 2D-Transmonqubits. **Microsoft** setzt auf topologische Quantencomputer und ist zu diesem Zweck mehrere Kooperationen mit Forschungseinrichtungen (z.B. University of Copenhagen, TU Delft) eingegangen. **IonQ** und **Honeywell** setzen auf Ionenfallen und **Xanadu** auf Photonen.

In Europa sind die Entwicklungen noch am Anfang und deren Potenzial schwer einzuschätzen. Erwähnenswert sind hierbei **IQM** und **Alpine Quantum Technologies** (AQT). IQM kommt aus Finnland mit deutscher Niederlassung in München und arbeitet mit supraleitenden Qubits. Darüber hinaus verfolgt die Firma einen Hardware-Software-Codesign-Ansatz. AQT ist in Innsbruck ansässig und entspringt dem Umfeld des Instituts für Quantenoptik und Quanteninformation (IQOQI). Sie setzten auf Ionenfallen.

In Deutschland gibt es ein paar Ideen für Start-ups, welche Quantencomputer bauen möchten und dafür Investoren oder Förderung suchen. Da jedoch weder Ergebnisse vorliegen noch deren Personal für herausragende Forschung bekannt ist, ist eine Einschätzung des Potenzials nicht möglich.

5.2.2 Forschung

Aufgrund der Fülle der Akteure in der Quantencomputerhardwareforschung belassen wir es hier bei einer schlichten Aufzählung der wichtigsten Akteure. Für Kurzbeschreibungen der meisten hier genannten Forschungseinrichtungen siehe Kapitel 20 der BSI-Studie [Wil+20].

USA National Institute of Standards of Technology (NIST), Boulder und Gaithersburg •

Einrichtungen des Departement of Energy, wie Lawrence Livermore, Sandia oder Los Alamos • Joint Quantum Institute, Maryland • MIT Lincoln Laboratory, Boston • Wisconsin Quantum Institute, Madison • Yale Quantum Institute, New Haven • Berkeley Quantum Information & Computation Center, Berkeley.

Kanada Institute for Quantum Computing, University of Waterloo • Équipe de Recherche en Physique de l'Information Quantique, Université de Sherbrooke • University of British Columbia (Raußendorf), Vancouver

Vereinigtes Königreich Sussex Centre for Quantum Technologies, Brighton • Oxford Quantum, Oxford • London Centre for Nanotechnology (LCN), London • Joint Quantum Centre, Durham-Newcastle • Centre for Quantum Photonics, Bristol

Schweiz Quantum Engineering Center, ETH Zürich • Basel Center for Quantum Computing and Quantum Coherence (QC2), Basel

Europäische Union QuTech, TU Delft, Niederlande • Institut für Quantenoptik und Quanteninformation (IQOQI), Innsbruck und Wien, Österreich • Commissariat à l'énergie atomique et aux énergies alternatives (CEA) Saclay und Grenoble, Frankreich • Centre national de la recherche scientifique (CNRS), Frankreich • Center for Quantum Devices (QDev), Copenhagen, Dänemark • Linnaeus Centre on Engineered Quantum Systems (Linneqs), Chalmers University of Technology, Schweden.

Deutschland Aachen Research Alliance (JARA) - Institut für Quanteninformation, Aachen • Max Planck-Institute for Quantum Optics (MPQ), Garching • Quantenbit Arbeitsgruppe, Schmidt-Kaler, Mainz • Arbeitgruppe Ospelkaus, Institut für Quantenoptik, Hannover • Arbeitgruppe Wunderlich, Universität Siegen • Forschungszentrum Jülich, Peter Grünberg Institut • Arbeitsgruppe Filipp, Walter-Meißner Institut, München

5.3 Algorithmen und Software

5.3.1 Industrie

Auch was die Software- und Algorithmenentwicklung für Quantencomputer angeht, ist Nordamerika führend. Zunächst entwickeln die großen Hardwareanbieter wie **Google**, **IBM**, **D-Wave** und **Rigetti** sowohl Open-Source-Softwarebibliotheken als auch neue Algorithmen für NISQ-Maschinen. Darüber hinaus gibt es eine Reihe von Start-ups, die Softwa-

re, Algorithmen und Beratungsleistungen anbieten. Dazu zählen in Nordamerika **QC Ware**, **Zapata Computing**, **1Qbit** und **QxBranch**. Ein Europa scheinen insbesondere **HQS** und **Cambridge Quantum Computing (CQC)** relevant. **Microsoft** spielt traditionell eine starke Rolle in der Algorithmusentwicklung auch jenseits topologischer Quantencomputer als Zielplattform. Sie setzen in ihren heutigen Dienstleistungen, wie die zuvor genannten Start-ups, auch auf quanten-inspirierte, klassische Algorithmen.

5.3.2 Forschung

In Nordamerika gibt es eine Reihe starker Grundlagenforscher für Quantencomputeralgorithmen. Dies sind unter anderem **MIT** (Lloyd), **University of Texas at Austin** (Aaronson), **University of New Mexico** (Crosson), **University of Toronto** (Aspuru-Guzik), **Berkeley Quantum Information & Computation Center, Berkeley** (Whaley, Vazirani), **University of Southern California** (Lidar) und das **NASA Quantum Artificial Intelligience Laboratory (QuAIL)** (Rieffel). Auf die NASA-QuAIL-Gruppe gehen wir in Abschnitt 5.6 noch genauer ein.

Im Vereinigten Königreich gibt es traditionell sehr starke Grundlagenforscher für Quantencomputeralgorithmen. Unter anderem sind dies **University of Oxford**, **University College London (UCL)** und das **Joint Quantum Centre, Durham-Newcastle**.

In der europäischen Union ist insbesondere das **Research Center for Quantum Software (QuSoft)** zu nennen. Hier gibt es eine starke Konzentration von weltweit führenden Experten auf dem Gebiet. An der **Universität Innsbruck** gibt es starke Theoriegruppen, die sich zunehmen auch mit NISQ-Algorithmen beschäftigen, z.B. die Gruppe von Wolfgang Lechner.

In Deutschland gibt es starke Grundlagenforscher an der **Universität zu Köln** (Gross), **FU Berlin** (Eisert), **FZ Jülich** (Wilhelm-Mauch, Michielsen) und **TU München** (König). Zusätzlich zu ihrem Hauptfokus widmen sich diese Forschergruppen zunehmend auch anwendungsorientierter Forschung. Neben diesen erfahren Forschergruppen richten eine Reihe von Arbeitsgruppen aus der Informatik ohne langjährige Erfahrung ihren Fokus auf Quantencomputeralgorithmen und Software. Dies sind unter anderem **Universität der Bundeswehr, München**, **Fraunhofer Gesellschaft**, **Universität Stuttgart** (Leymann), und **LMU** (Linnhoff-Popien). Diese Aktivitäten beschränken sich größtenteils auf die Abbildung von Anwendungen sowie die Programmierung von Quantencomputern.

5.4 Potentielle Endanwender

Aufgrund des großen Interesses am Thema Quantencomputing mangelt es mittlerweile nicht mehr an interessierten möglichen Endanwendern für Quantencomputern aus der Industrie. Insbesondere größere Unternehmen können es sich leisten, in begrenztem Umfang Forschungsaktivitäten auf diesem Gebiet zu betreiben, um für mögliche Durchbrüche in der Technologie gewappnet zu sein. Dies sind in Deutschland zum Beispiel **VW**, **BMW**, **Daimler**, **Bosch**, **Siemens**, **Zeiss**, **Airbus**, **SAP**, **E.on**, **Deutsche Telekom**, **Deutsche Bahn**, **Bayer**, **Merck**, **Boehringer Ingelheim**, **Covestro** und **BASF**. Viele dieser Unternehmen unterhalten kleinere Forschergruppen zu diesem Zweck und kooperieren kostenpflichtig mit Hardwareherstellern und Software-Start-ups. Zudem organisieren sich diese Firmen in Interessengruppen wie die **Quantum Computing Industry Group**[1] in Deutschland oder dem **Quantum Industry Consortium (QuIC)** in Europa. Aufgrund des frühen Stadiums der Entwicklung tauschen sich die Unternehmen noch relativ offen aus.

5.5 Wirtschaftlichkeitsanalyse

Laut den Autoren der Studie der Deutschen Akademie der Technikwissenschaften [Kag+20] wird Quantencomputern ein größeres Marktpotenzial zugetraut als allen anderen Quantentechnologien. Sie schreiben „Für den Quantencomputer wird mittel- und langfristig ein Marktpotenzial von bis zu dreistelligen Milliardenbeträgen prognostiziert. Durch die vielfältigen Anwendungsmöglichkeiten entlang der Wertschöpfungskette ist zudem ein sehr großes sekundäres Wertschöpfungspotenzial vorhanden. Es entsteht zurzeit weltweit ein Ökosystem aus Hard- und Software- sowie Mischanbietern. Deutsche und europäische Firmen fehlen jedoch vor allem im Hardwarebereich.“ [Kag+20].

Es ist schwierig, genaue Prognosen zu erstellen, und die Schätzungen variieren stark (siehe [Kag+20] und Abbildung 5.1). Die größte Wertschöpfung wird nicht in der Bereitstellung von Hardware erwartet sondern in deren Nutzung. Dies erklärt auch das Vorgehen der meisten Hardwarehersteller (z.B. IBM) mittels exklusiven Kooperationsverträgen sicherzustellen, dass sie Rechte an den entwickelten Anwendungen behalten. Zudem stellt dies eine weitere Hürde für die industrielle Quantencomputerhardwareentwicklung in Deutschland und Europa dar. Diese lässt sich vermutlich nur umsetzen, falls deutsche und europäische Hardwarehersteller massive Subventionen erhalten und auf ein Geschäftsmodell setzten, das die Teilhabe an der weiteren Wertschöpfungskette beinhaltet. Für weitere Details

[1] Der Autor ist Mitglied in dieser Gruppe

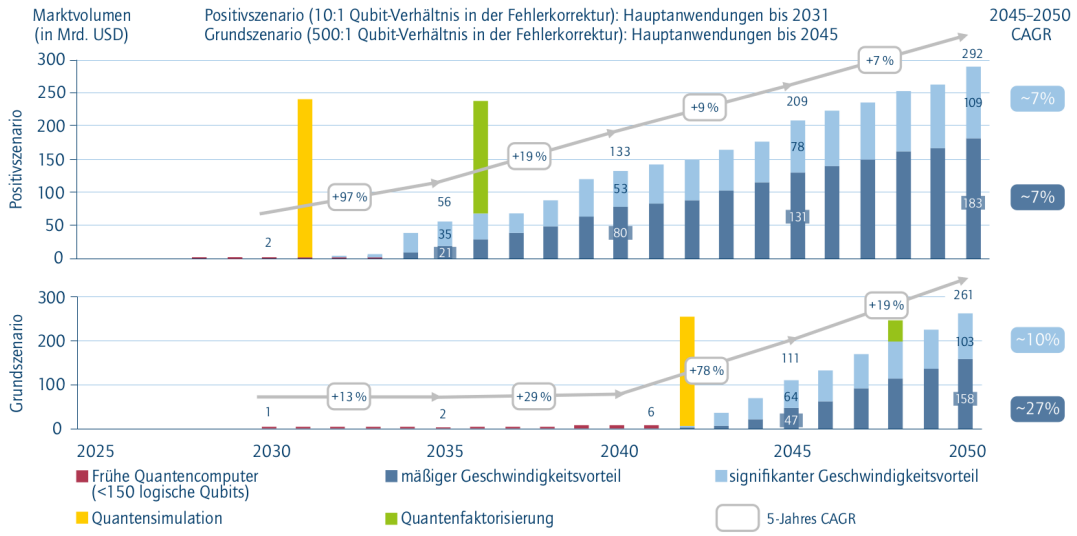

Abbildung 5.1: **"Projizierte Entwicklung des Marktpotenzials für Quantencomputer (2025–2050) mit Grund- und Positivszenarios" [Kag+20] (Originalquelle [Gro18]).**

zum Marktpotenzial verweisen wir auf Abschnitt 8.2 in [Kag+20] und die darin zitierten Studien.

5.6 Rolle des DLR

Wie in den vorherigen Abschnitten beschrieben, gibt es in Deutschland starke Grundlagenforscher aus den Bereichen Algorithmen- und Hardwareforschung. Demgegenüber stehen eine Vielzahl von möglichen Endanwendern und einige Serviceanbieter, die an Anwendungen für Quantencomputer interessiert sind. Es fehlt jedoch an Akteuren, die die Lücke zwischen den beiden zuvor genannten Gruppen schließen können, den *Brückenbauern*.

Um das Marktpotenzial voll auszuschöpfen, muss darauf hingearbeitet werden, souveränen Zugriff auf Quantencomputerhardware sicherzustellen und die Entwicklung mitzugestalten. Dazu kann und sollte die Anschaffung nordamerikanischer Quantencomputer nur begleitend sein. Darüber hinaus sollte die Quantencomputerhardwareentwicklung in Deutschland und Europa auf industriellem Niveau vorangetrieben werden. Diese sollte

in enger Zusammenarbeit mit Algorithmen- und Softwareentwicklern im Rahmen eines Hardware-Software-Codesigns vorangetrieben werden.

Das DLR könnte sowohl im Hardware- als auch im Softwarebereich einer der Brückenbauer sein. Zunächst könnte die Expertise in angrenzenden Quantentechnologiebereichen genutzt werden, um die Hardwareentwicklung voranzutreiben. Idealerweise könnte dies in Zusammenarbeit mit europäischen Hardwareherstellern geschehen. Diese Bemühungen könnte das DLR außerdem mit der Entwicklung von hardwarenahen Algorithmen und Software begleiten. Dazu lohnt sich ein Blick auf die Ausrichtung der NASA QuAIL-Gruppe, die seit Jahren eine anwendungsorientierte und gleichzeitig hardwarenahe Strategie inklusive Zusammenarbeit mit Hardwareherstellern verfolgt. Die Gruppe arbeitet an Algorithmen und Software, zeichnet sich jedoch durch enge Zusammenarbeit mit Hardwareherstellern wie D-Wave, Google und Rigetti aus. Intensiven Austausch (auch von Personal) und exklusiven Zugriff auf die Maschinen ermöglicht es der QuAIL-Gruppe die Entwicklung mit Fokus auf Anwendungsrelevanz mitzugestalten. Der Anwendungsfokus der NASA-Gruppe geht über Luft- und Raumfahrtanwendungen hinaus, da sich die Gruppe als Brückenbauer der Forschung zu Quantencomputeranwendungen versteht und damit die sich gerade entwickelnde Fachindustrie unterstützt.

Zumindest was die Softwareseite betrifft, könnte das DLR die Strategie der amerikanischen Luft- und Raumfahrtforschungseinrichtung NASA folgen und mit dieser Zusammenzuarbeiten. Dabei könnte es auf die Erfahrung des Instituts for Softwaretechnologie zurückgreifen, welches schon seit 2015 mit NASA QuAIL zusammenarbeitet. Denkbar wäre zum Beispiel eine gemeinsame Softwareentwicklung mit NASA QuAIL. Dazu gibt es bereits grundsätzliche Übereinkünfte zwischen dem DLR und der NASA und eine Umsetzung in kleinem Rahmen wurde in die Wege geleitet. Durch eine Zusammenarbeit in größeren Rahmen könnte das gesamte DLR stark von der Experise der NASA QuAIL Gruppe profitieren, während das Institut für Softwaretechnologie im Gegenzug die Softwareexpertise liefern könnte, die bei NASA QuAIL benötigt wird.

Ein entscheidender Unterschied zwischen DLR und NASA ist jedoch der Hardwarezugriff. Hier müssten die nordamerikanischen Hardwarehersteller durch europäische Akteure ergänzt werden, mit denen offen zusammengearbeitet wird. Da die europäische Industrie bisher lediglich wenige experimentelle Quantencomputer-Hardware mit unklarer Anwendungsreife vorweisen kann, macht es Sinn, dass auch Forschungseinrichtungen die Hardware-Entwickler-Rolle übernehmen. Deren Prototypen könnten dann idealerweise von Unternehmen weiterentwickelt werden. Das DLR könnte eine dieser Forschungseinrichtungen sein. Aufgrund des technologischen Vorsprungs der nordamerikanischen Hersteller ist es sinnvoll, parallel zur eigenen Hardwareentwicklung Zugriff bei diesen Herstellern einzukaufen.

In diesem Zusammenhang erscheint das Vorgehen des FZ Jülich sinnvoll. Dort wird eine einheitliche Plattform für den offenen Zugang zu verschiedenen Quantencomputerhardwareplattformen (JUNIQ) geschaffen. Die Plattformen umfassen kommerzielle und experimentelle Maschinen sowie Simulatoren. Idealerweise würde das DLR seine Bemühungen in ein solches Vorhaben integrieren. Dies erscheint umso attraktiver, da um das FZ Jülich viele Experten zum Thema vereint sind. Mit einigen dieser Experten (Wilhelm-Mauch, Michielsen, Gross) arbeitet das Institut für Softwaretechnologie bereits seit mehreren Jahren zusammen. Die Hardwareentwicklungen in Jülich beinhalten jedoch nur Festkörperplattformen. Diese Lücke könnte das DLR mit atomistischen Plattformen schließen.

Aufgrund der Vielzahl an möglichen Endanwendern aus der Industrie erscheint es nicht erstrebenswert, dass das DLR sich als einer unter vielen möglichen Endanwendern einreiht. Eine vielversprechende Rolle für das DLR wäre die des Brückenbauers und Vorreiters für eine neue Technologie gemäß dem DLR-Motto "Wissen für Morgen".

Literatur

[Sho94] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, S. 124–134. DOI: 10.1109/SFCS.1994.365700.

[Fey86] Richard P. Feynman. "Quantum mechanical computers". In: *Foundations of Physics* 16.6 (1986), S. 507–531. ISSN: 1572-9516. DOI: 10.1007/BF01886518. URL: https://doi.org/10.1007/BF01886518.

[DJ92] David Deutsch und Richard Jozsa. "Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992), S. 553–558. DOI: 10.1098/rspa.1992.0167. URL: https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1992.0167.

[Gro96] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866. URL: https://doi.org/10.1145/237814.237866.

[Wil+20] Frank K. Wilhelm u. a. *Status of quantum computer development*. Studie. Bundesamt für Sicherheit in der Informationstechnik, 2020. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_2.pdf.

[Kag+20] Henning Kagermann u. a. *Innovationspotenziale der Quantentechnologien der zweiten Generation*. Studie. Deutsche Akademie der Technikwissenschaften, 2020. URL: https://www.acatech.de/publikation/innovationspotenziale-der-quantentechnologien/.

[NC11] Michael A. Nielsen und Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. USA: Cambridge University Press, 2011. ISBN: 1107002176.

[KN98] Tadashi Kadowaki und Hidetoshi Nishimori. "Quantum annealing in the transverse Ising model". In: *Phys. Rev. E* 58 (5 1998), S. 5355–5363. DOI: 10.1103/PhysRevE.58.5355. URL: https://link.aps.org/doi/10.1103/PhysRevE.58.5355.

[Far+00] Edward Farhi u. a. "Quantum Computation by Adiabatic Evolution". In: *arXiv e-prints*, quant-ph/0001106 (Jan. 2000), quant–ph/0001106. arXiv: quant-ph/0001106 [quant-ph].

[Den+16] Vasil S. Denchev u. a. "What is the Computational Value of Finite-Range Tunneling?" In: *Phys. Rev. X* 6 (3 2016), S. 031015. DOI: 10.1103/PhysRevX.6.031015. URL: https://link.aps.org/doi/10.1103/PhysRevX.6.031015.

[LB99] Seth Lloyd und Samuel L. Braunstein. "Quantum Computation over Continuous Variables". In: *Phys. Rev. Lett.* 82 (8 1999), S. 1784–1787. DOI: 10.1103/PhysRevLett.82.1784. URL: https://link.aps.org/doi/10.1103/PhysRevLett.82.1784.

[Pfi19] Olivier Pfister. "Continuous-variable quantum computing in the quantum optical frequency comb". In: *Journal of Physics B: Atomic, Molecular and Optical Physics* 53.1 (2019), S. 012001. DOI: 10.1088/1361-6455/ab526f. URL: https://doi.org/10.1088/1361-6455/ab526f.

[RBB03] Robert Raussendorf, Daniel E. Browne und Hans J. Briegel. "Measurement-based quantum computation on cluster states". In: *Phys. Rev. A* 68 (2 2003), S. 022312. DOI: 10.1103/PhysRevA.68.022312. URL: https://link.aps.org/doi/10.1103/PhysRevA.68.022312.

[DI00] David P. DiVincenzo und IBM. "The Physical Implementation of Quantum Computation". In: *arXiv:0002077 [quant-ph]* (2000). URL: https://arxiv.org/abs/quant-ph?0002077.

[Mol+18] Nikolaj Moll u. a. "Quantum optimization using variational algorithms on near-term quantum devices". In: *Quantum Science and Technology* 3.3 (2018), S. 030503. DOI: 10.1088/2058-9565/aab822. URL: https://doi.org/10.1088/2058-9565/aab822.

[HHL09] Aram W. Harrow, Avinatan Hassidim und Seth Lloyd. "Quantum Algorithm for Linear Systems of Equations". In: *Phys. Rev. Lett.* 103 (15 2009), S. 150502. DOI: 10.1103/PhysRevLett.103.150502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.103.150502.

[HV03] Ramesh Hariharan und V. Vinay. "String matching in $\tilde{\mathcal{O}}(\sqrt{n}+\sqrt{m})$ quantum time". In: *J. Discrete Algorithms* 1 (Jan. 2003), S. 103–110.

[Mon17] Ashley Montanaro. "Quantum Pattern Matching Fast on Average". In: *Algorithmica* 77.1 (2017), S. 16–39. ISSN: 1432-0541. DOI: 10.1007/s00453-015-0060-4. URL: https://doi.org/10.1007/s00453-015-0060-4.

[Qua] *Quantum Algorithm Zoo*. https://quantumalgorithmzoo.org/. Accessed: 2020-12-29.

[FGG14] Edward Farhi, Jeffrey Goldstone und Sam Gutmann. "A Quantum Approximate Optimization Algorithm". In: *arXiv e-prints*, arXiv:1411.4028 (Nov. 2014), arXiv:1411.4028. arXiv: 1411.4028 [quant-ph].

[Bia+17] Jacob Biamonte u. a. "Quantum machine learning". In: *Nature* 549.7671 (2017), S. 195–202. ISSN: 1476-4687. DOI: 10.1038/nature23474. URL: https://doi.org/10.1038/nature23474.

[NT17] Hidetoshi Nishimori und Kabuki Takada. "Exponential Enhancement of the Efficiency of Quantum Annealing by Non-Stoquastic Hamiltonians". In: *Frontiers in ICT* 4 (2017), S. 2. ISSN: 2297-198X. DOI: 10.3389/fict.2017.00002. URL: https://www.frontiersin.org/article/10.3389/fict.2017.00002.

[ONL18] Masaki Ohkuwa, Hidetoshi Nishimori und Daniel A. Lidar. "Reverse annealing for the fully connected *p*-spin model". In: *Phys. Rev. A* 98 (2 2018), S. 022314. DOI: 10.1103/PhysRevA.98.022314. URL: https://link.aps.org/doi/10.1103/PhysRevA.98.022314.

[CJS13] B. D. Clader, B. C. Jacobs und C. R. Sprouse. "Preconditioned Quantum Linear System Algorithm". In: *Phys. Rev. Lett.* 110 (25 2013), S. 250504. DOI: 10.1103/PhysRevLett.110.250504. URL: https://link.aps.org/doi/10.1103/PhysRevLett.110.250504.

[Zac19] Christopher Zachow. *THE QLS ALGORITHM FOR RADAR CROSS SECTION CALCULATION*. 2019. URL: https://elib.dlr.de/132821/.

[Lub+20] Michael Lubasch u. a. "Variational quantum algorithms for nonlinear problems". In: *Phys. Rev. A* 101 (1 2020), S. 010301. DOI: 10.1103/PhysRevA.101.010301. URL: https://link.aps.org/doi/10.1103/PhysRevA.101.010301.

[WBL12] Nathan Wiebe, Daniel Braun und Seth Lloyd. "Quantum Algorithm for Data Fitting". In: *Phys. Rev. Lett.* 109 (5 2012), S. 050505. DOI: 10.1103/PhysRevLett.109.050505. URL: https://link.aps.org/doi/10.1103/PhysRevLett.109.050505.

[Pap+14] Giuseppe Davide Paparo u. a. "Quantum Speedup for Active Learning Agents". In: *Phys. Rev. X* 4 (3 2014), S. 031002. DOI: 10.1103/PhysRevX.4.031002. URL: https://link.aps.org/doi/10.1103/PhysRevX.4.031002.

[Ami+18] Mohammad H. Amin u. a. "Quantum Boltzmann Machine". In: *Phys. Rev. X* 8 (2 2018), S. 021050. DOI: 10.1103/PhysRevX.8.021050. URL: https://link.aps.org/doi/10.1103/PhysRevX.8.021050.

[CCL19] Iris Cong, Soonwon Choi und Mikhail D. Lukin. "Quantum convolutional neural networks". In: *Nature Physics* 15.12 (2019), S. 1273–1278. ISSN: 1745-2481. DOI: 10.1038/s41567-019-0648-8. URL: https://doi.org/10.1038/s41567-019-0648-8.

[Gro18] The Boston Consulting Group. *The Coming Quantum Leap in Computing*. Techn. Ber. 2018. URL: https://www.bcg.com/en-gb/publications/2018/coming-quantum-leap-computing.