



Quantenzeitalter

*Quantencomputing als Gamechanger
für Finanz- und Realwirtschaft*

„Quantencomputing ist der nächste technologische Durchbruch, der die Welt verändern wird.“

Ginni Rometty, ehemalige CEO von IBM

„Quantencomputer sind der Schlüssel zur Entschlüsselung der Geheimnisse des Universums.“

Seth Lloyd, Professor für Maschinenbau am MIT

„Quantencomputer werden uns helfen, Probleme zu lösen, die für klassische Computer unlösbar sind.“

David Deutsch, Physiker an der Universität Oxford

„Die Quantenwelt eröffnet uns eine völlig neue Dimension der Informationsverarbeitung.“

Hartmut Neven, Leiter des Quantum Artificial Intelligence Lab bei Google

„Quantencomputing wird uns helfen, die komplexesten Probleme der Welt zu lösen, von der Klimamodellierung bis zur Optimierung von Lieferketten.“

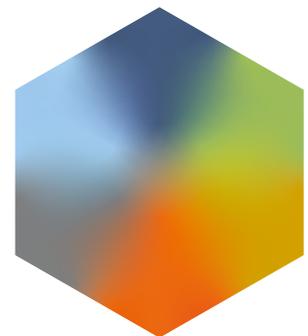
Arvind Krishna, CEO von IBM

„Die Quantenrevolution wird jeden Aspekt unseres Lebens beeinflussen, von der Gesundheitsversorgung bis zur Finanzwelt.“

Chad Rigetti, Gründer von Rigetti Computing

„Die Zukunft der Kryptographie liegt in der Quantenwelt.“

Peter Shor, Mathematiker am MIT



**Erkennen
ist mehr
als Sehen**

Bad Homburg/Sankt Gallen, November 2024

Vorwort

Liebe Leserinnen und Leser,

erst seit kurzem ist die Welt mit den rasanten Fortschritten und explosiven Entwicklungssprüngen der generativen Künstlichen Intelligenz konfrontiert. Doch schon zeichnet sich ein neuer „Gamechanger“ ab, der bisherige Grundlagen der Digitalisierung vollständig verändern wird: *Quantencomputer!*

Diese neuartige Technologie nutzt spezielle Eigenschaften der Quantenphysik und ermöglicht so ein Vielfaches der maximalen Rechenleistung heutiger *Supercomputer*. Noch befinden sich Quantencomputer in der Experimentierphase. Doch bereits in wenigen Jahren könnten skalierbare Quantencomputer Realität sein. Auch ein „*Quanten-Internet*“ liegt dann im Bereich des Möglichen.

Schon heute investieren Tech-Giganten wie *IBM, Google, Microsoft, Amazon* und *Intel* massiv in die Quantentechnologie, die enorme Vorteile in wichtigen Anwendungsgebieten verspricht. Das Rennen um die Vorherrschaft bei dieser revolutionären Zukunftstechnologie ist in vollem Gang – mit den USA, Europa und China als Hauptakteuren.

Die rasant zunehmende Dynamik zeigt klar: Die strategische Bedeutung dieser Technologie ist enorm – auch aus geopolitischer Perspektive. Denn Quantencomputer haben das Potential, ganze Industrien zu innovieren und neue Zukunftsmärkte in der Real- und Finanzwirtschaft zu erschaffen. Gleichzeitig wären sie in der Lage, selbst hocheffektive Verschlüsselungsverfahren zu durchbrechen.

Generell versprechen Quantencomputer Durchbrüche in der Analyse und Optimierung komplexer Rechenprobleme, die mit klassischen Computern kaum lösbar sind. Das Anwendungsspektrum reicht von Kryptographie und Materialwissenschaften über Medizin und Pharmaentwicklung bis zu Logistik und Raumfahrt. Auch im Finanzsektor eröffnen sich zahlreiche neue Horizonte.

Das Phänomen *Quantencomputer* wird vom *FERI Cognitive Finance Institute* bereits seit 2019 intensiv analysiert. Angesichts wichtiger technologischer Durchbrüche im Jahr 2024 erscheint es nun aber geboten, den neuesten Stand der Quantencomputer zu beleuchten und das disruptive Potential dieser Technologie klar herauszuarbeiten.

Unternehmer und Investoren sollten diese Entwicklung – die nicht nur enorme Chancen, sondern auch völlig neue Risiken mit sich bringt – in den kommenden Jahren sehr genau im Blick behalten.

Wir wünschen eine disruptive und erkenntnisreiche Lektüre!



Dr. Heinz-Werner Rapp

Gründer & Leiter Steering Board
FERI Cognitive Finance Institute



Dr. Michael Blaschke

Global Principal IT Architect, Experte für Institutional DLT,
Unternehmensberater für Technologiestrategie
Podcast Co-Host „Bitcoin, Fiat & Rock’n’Roll“

Inhalt

1	<i>Executive Summary</i>	3
2	<i>Einführung in die Quantentechnologie</i>	5
2.1	Definition und grundlegende Prinzipien der Quantentechnologie	7
2.2	Vergleich mit klassischer Computertechnologie	9
2.3	Potentielle Anwendungen und Vorteile der Quantentechnologie	11
2.4	Adaptionszyklus	11
3	<i>Quantentechnologie</i>	14
3.1	Quantenbits (Qubits) und ihre Eigenschaften	14
3.2	Quantengatter und Operationen	15
3.3	Quantenalgorithmen und Protokolle	15
3.4	Quantenfehlerkorrektur und Fehlertoleranz	15
4	<i>Aktueller Stand der Quantentechnologie</i>	16
4.1	Überblick über bestehende Plattformen für Quantentechnologie	16
4.2	Herausforderungen und Einschränkungen in der Quantentechnologie	16
4.3	Aktuelle Fortschritte und Durchbrüche auf dem Gebiet	17
5	<i>Quantentechnologie in der Praxis</i>	19
5.1	Anwendungsfälle und praktische Anwendungen von Quantentechnologie	19
5.2	Praktische Überlegungen für die Implementierung von Quantentechnologie	22
5.3	Mögliche Quantum-Auswirkungen auf die Kryptographie	22
5.3.1	Kryptographie in heutigen Finanzsystemen	23
5.3.2	Quantenbedrohung für herkömmliche Kryptographie	24
6	<i>Quantentechnologie für Investoren</i>	27
6.1	Investitionsmöglichkeiten in der Quantentechnologie-Branche	27
6.2	Markttrends und Wachstumspotential	27
6.3	Risiken und Herausforderungen für Investoren in der Quantentechnologie	28
6.4	Die geopolitische Dimension des Quantencomputing	29
6.4.1	Investitionen in Forschung und Entwicklung	29
6.4.2	Anwendungen und Patente	30
6.4.3	Internationale Zusammenarbeit und Wettbewerb	31
6.4.4	Herausforderungen und Zukunftsaussichten	32
7	<i>Fazit und Ausblick auf die Zukunft</i>	33
7.1	Implikationen der Quantentechnologie für Realwirtschaft und Finanzmärkte	33
7.2	Prognosen für die Zukunft der Quantentechnologie	36
7.3	Handlungsempfehlungen: Quantencomputing für Praktiker und Investoren	37
	Erläuterungen	39
	Literaturverzeichnis	40

Abbildungsverzeichnis

Abb. 1:	Entwicklung der Quantencomputertechnik im Laufe der Zeit	6
Abb. 2:	Computing, Kommunikation und Sensorik als Teilbereiche der Quantentechnologie	7
Abb. 3:	Auswirkungen der Quanteninformatik	10
Abb. 4:	Zunehmende Aufmerksamkeit und FuE-Aktivitäten im Bereich Quantencomputer	12
Abb. 5:	Quantencomputer und Finanzen: Google Scholar Ergebnisse	13
Abb. 6:	Tempo der Entwicklung im Vergleich zu den individuellen Erwartungen	13
Abb. 7:	Quantenbits (Qubits)	14
Abb. 8:	Industrieübergreifende Schlüsselanwendungen des Quantencomputing	20
Abb. 9:	Potentielle Vorteile des Quantencomputing im Finanzsektor	22
Abb. 10:	Unterschied zwischen symmetrischer und asymmetrischer Schlüsselverschlüsselung	23
Abb. 11:	Benötigte Investitionsschwerpunkte zur Förderung des Quantencomputing	27
Abb. 12:	Führende Länder und Regionen der Quantentechnologie	30
Abb. 13:	Die Schlüsseltechnologien des Quantencomputing	34
Abb. 14:	Erwartete Durchsetzungszeit für Quantencomputer	37

Tabellenverzeichnis

Tab. 1:	Ausgewählte Durchbrüche im Quantencomputing	17
Tab. 2:	Risiken und Herausforderungen für Investoren	28

Abstract (KI-generiert)*

Zusammenfassung: „Quantenzeitalter: Quantencomputing als Gamechanger für Finanz- und Realwirtschaft“

Die Analyse beleuchtet die bahnbrechenden Möglichkeiten, die Quantencomputer für verschiedene Branchen bieten, und geht dabei besonders auf innovative Anwendungen und die Herausforderungen im Bereich der Verschlüsselung ein.

Kernpunkte:

1. Innovative Anwendungen: Quantencomputer nutzen die Prinzipien der Quantenmechanik, um Berechnungen viel schneller durchzuführen als klassische Computer. Diese Technologie könnte in der Arzneimittelforschung, Logistik und Finanzwirtschaft sowie den Materialwissenschaften zu erheblichen Fortschritten führen. Beispielsweise können Quantencomputer komplexe Molekülstrukturen analysieren, was die Entwicklung neuer Medikamente beschleunigt. In der Logistik könnten sie die Optimierung von Lieferketten revolutionieren.

2. Vorteile im Finanzsektor: Im Finanzwesen versprechen Quantenalgorithmen Verbesserungen bei der Portfoliooptimierung, dem Risikomanagement und der Betrugserkennung. Diese Anwendungen könnten die Effizienz und Genauigkeit von Finanzanalysen erheblich steigern.

3. Herausforderungen in der Verschlüsselung: Quantencomputer stellen eine Bedrohung für die derzeitigen Verschlüsselungsmethoden dar, da sie in der Lage sein könnten, gängige kryptographische Algorithmen wie RSA und Elliptic Curve Cryptography (ECC) zu knacken. Dies gefährdet die Sicherheit von Online-Transaktionen und sensiblen Daten.

4. Lösungsansätze für die Sicherheit: Um diesen Bedrohungen zu begegnen, wird an quantensicheren Verschlüsselungsmethoden gearbeitet, die auch gegen Angriffe von Quantencomputern resistent sind. Diese neuen Methoden müssen entwickelt und implementiert werden, um die Sicherheit von Finanzsystemen und anderen kritischen Infrastrukturen zu gewährleisten.

5. Zukunftsperspektiven: Die Entwicklung von Quantencomputern erfordert eine Anpassung der Kryptographie-Standards. Unternehmen und Regierungen investieren in die Forschung und Entwicklung von Post-Quantum-Kryptographie, um zukünftige Sicherheitsrisiken zu minimieren.

Insgesamt zeigt die Analyse, dass Quantencomputing das Potential hat, zahlreiche Branchen zu transformieren, während es gleichzeitig neue Herausforderungen im Bereich der Datensicherheit mit sich bringt. Die Entwicklung quantensicherer Verschlüsselungstechnologien ist entscheidend, um die Integrität und Vertraulichkeit von Daten in der Zukunft zu schützen.

* KI-generierte Zusammenfassung der vorliegenden Analyse durch *FERI MAI* (eigene KI-Anwendung), (Prompt: Du bist ein Journalist mit guten Technikenntnissen. Bitte schreibe eine Zusammenfassung des Textes, der auch für Laien gut verständlich ist. Berücksichtige dabei besonders die zahlreichen innovativen Anwendungsmöglichkeiten, aber auch das Thema Verschlüsselung, 05.11.2024)

1 Executive Summary

- Technologische Durchbrüche im Quantencomputing führen zu bahnbrechenden Fortschritten in der **Datenverarbeitung**, zu revolutionären Anwendungen in der Arzneimittelforschung und der Kryptographie sowie zur Lösung komplexer Optimierungsprobleme in verschiedenen Branchen.
- Im Vergleich zu klassischen Computern ermöglichen Quantencomputer durch die Nutzung von Qubits anstelle von Bits eine **exponentiell höhere Rechenleistung**. Während klassische Computer sequentiell arbeiten, nutzen Quantencomputer die Prinzipien der Superposition und Verschränkung, um viele Berechnungen *gleichzeitig* zu verarbeiten. Dies bedeutet, dass sie in der Lage sind, Probleme zu lösen, die für klassische Computer zeitaufwändig sind. Beispielsweise können Quantencomputer komplexe Molekülstrukturen in der Arzneimittelforschung analysieren und so die Entwicklung neuer Medikamente erheblich beschleunigen.
- Zusätzlich bieten Quantencomputer neue **Möglichkeiten in der Kryptographie**, indem sie nahezu unüberwindbare **Verschlüsselungsmethoden** ermöglichen, was besonders für die Sicherheit von Online-Transaktionen von hoher Bedeutung ist.
- Aktuelle Systeme demonstrieren bereits, dass Quantencomputer in der Lage sind, bestimmte Aufgaben oder Berechnungen effizienter und schneller zu lösen als klassische Computer. Kontinuierliche Fortschritte bei der **Qubit-Stabilität**, **Fehlerkorrektur** und **Skalierbarkeit** beschleunigen die Entwicklung. Der Fokus liegt derzeit auf hybriden klassisch-quantenmechanischen Systemen als Übergangslösung.
- Die Marktentwicklung und Investitionslandschaft im Quantencomputing-Sektor zeigen ein beeindruckendes Wachstum. Prognosen sehen den globalen Markt bis 2030 bei 65 Mrd. USD, mit einer jährlichen Wachstumsrate von 56 %. Venture Capital-Investitionen in Quantentechnologien erreichten 2023 2,4 Mrd. USD, ein Plus von 46 % gegenüber dem Vorjahr. Staatliche Förderprogramme in der EU, den USA und China investieren Milliarden in die Technologie. Gleichzeitig wächst die Zahl der Quantencomputing-Startups weltweit auf über 500, mit steigender Tendenz.
- Die Anwendungsbereiche mit hohem Disruptionspotential durch Quantencomputing sind vielfältig: Im **Finanzsektor** versprechen Quantenalgorithmien Durchbrüche in Portfoliooptimierung, Risikomanagement und Betrugserkennung. Die **Pharma- und Biotechnologiebranche** profitiert von präziseren Molekularsimulationen, effizientem Wirkstoffdesign und Fortschritten in der personalisierten Medizin. In **Luft- und Raumfahrt, Logistik und Lieferkettenmanagement** ermöglichen Quantencomputer optimierte Routen, verbessertes Bestandsmanagement und genauere Nachfrageprognosen. Auch in den Bereichen **Künstliche Intelligenz und Cybersicherheit** werden signifikante Fortschritte erwartet, von der Beschleunigung von Machine Learning bis hin zu quantensicheren Kryptographiemethoden.
- Das Ökosystem der Technologieführer im Quantencomputing ist vielfältig und dynamisch. Tech-Giganten wie *IBM, Google, Microsoft, Amazon* und *Intel* investieren massiv in die Entwicklung von Quantenhardware und -software. Spezialisierte Unternehmen wie *D-Wave, Rigetti, IonQ, PsiQuantum* und *Xanadu* treiben Innovationen in spezifischen Quantentechnologien voran. Renommierte Forschungsinstitutionen wie *MIT, Caltech, TU München* und die *Fraunhofer-Gesellschaft* leisten grundlegende wissenschaftliche Beiträge. Cloud-Quantencomputing-Anbieter wie *Amazon Braket, IBM Quantum Experience* und *Azure Quantum* demokratisieren den Zugang zu Quantenressourcen für Entwickler und Unternehmen weltweit.

- Trotz des enormen Potentials stehen dem Quantencomputing noch erhebliche Herausforderungen und Risiken gegenüber. Technische Hürden wie die **Verbesserung der Qubit-Kohärenz**, die **Skalierbarkeit der Systeme** und die Implementierung effektiver **Fehlerkorrekturmechanismen** müssen überwunden werden. Ein akuter Mangel an **interdisziplinären Quantenexperten** bremst die Entwicklung und Anwendung der Technologie. Regulatorische Unsicherheiten, insbesondere im Bereich von Exportkontrollen, Datenschutz und ethischen Richtlinien, schaffen ein komplexes Geschäftsumfeld. Zudem besteht die Gefahr überhöhter Erwartungen, die zu einer „Quantum Bubble“ mit unrealistischen Versprechungen führen könnten.
- Für Unternehmer ergeben sich klare strategische Empfehlungen, um von der Quantenrevolution zu profitieren. Zentral ist der **Aufbau von Quantencomputing-Kompetenz** im Unternehmen, gefolgt von der Identifikation und Priorisierung relevanter **Use Cases**. Partnerschaften mit Quantencomputing-Anbietern und Forschungseinrichtungen können den Wissenstransfer beschleunigen. Die Verfolgung **hybrider Lösungsansätze**, die klassische High-Performance-Computing-Systeme mit Quantenalgorithmen kombinieren, ermöglicht eine schrittweise Integration. Parallel dazu ist die Vorbereitung einer **quantenresistenten Sicherheitsinfrastruktur** unerlässlich, um zukünftige Bedrohungen durch Quantencomputer abzuwehren.
- Für Investoren bieten sich vielfältige Strategien und Opportunitäten im Quantencomputing-Sektor. Ein diversifiziertes Quantenportfolio sollte Hardware, Software, Anwendungen und Beratungsdienstleistungen umfassen. Frühe Investments in vielversprechende Quantencomputing-Startups können potentiell hohe Renditen erzielen, doch auch etablierte Tech-Unternehmen mit starkem Quantenengagement bieten interessante Investitionsmöglichkeiten.
- Der Zeithorizont für die Entwicklung des Quantencomputing erstreckt sich über die nächsten Jahrzehnte. Zwischen 2025 und 2027 werden die ersten kommerziellen Quantencomputer mit 100 bis 1'000 logischen Qubits erwartet. Von 2027 bis 2030 dürfte die Quantenüberlegenheit in breiteren Anwendungsfeldern demonstriert werden. Im Zeitraum 2030 bis 2035 werden fehlerkorrigierte Quantensysteme mit Millionen logischer Qubits prognostiziert. **Ab 2035 könnten skalierbare Quantencomputer** und ein „Quanten-Internet“ Realität werden.
- Auch für die Finanzwirtschaft ergeben sich durch Quantencomputing weitreichende Implikationen. Quantenalgorithmen versprechen ein optimiertes Portfoliomanagement und präzisere Risikobewertungen. Neue Anlageprodukte basierend auf Quantensimulationen und -vorhersagen könnten den Markt revolutionieren. Gleichzeitig steigen die Anforderungen an Cybersicherheit und Datenschutz, was eine Umstellung auf quantenresistente Kryptographiestandards notwendig macht. Langfristig könnten Quantencomputer sogar traditionelle Finanzmodelle und -theorien grundlegend in Frage stellen und neu definieren.
- Das globale Marktpotential für Quantentechnologien entwickelt sich dynamisch: Der Quantencomputing-Markt soll bis 2035 auf 28 bis 72 Mrd. EUR anwachsen, die Quantenkommunikation auf 11 bis 15 Mrd. EUR und die Quantensensorik auf 0,5 bis 2,7 Mrd. EUR. Insgesamt wird bis 2035 ein wirtschaftlicher Mehrwert von etwa 2 Bio. EUR erwartet, insbesondere in den Schlüsselbranchen Chemie, Biowissenschaften, Finanzen und Mobilität. Das Ökosystem umfasst derzeit 367 Startups weltweit. Die kumulierten privaten und Unternehmensinvestitionen belaufen sich auf 8,5 Mrd. EUR. Zusätzlich haben Regierungen weltweit bereits Fördermittel in Höhe von rund 42 Mrd. EUR zugesagt.
- Zusammenfassend lässt sich sagen, dass Quantencomputing an der **Schwelle zur kommerziellen Reife** steht und in den kommenden Jahren tiefgreifende Auswirkungen auf zahlreiche Branchen haben wird. Unternehmer und Investoren sollten proaktiv handeln, um von dieser transformativen Technologie zu profitieren und potentielle Risiken zu minimieren. Eine fundierte Strategie, gezielte Investitionen und der Aufbau von Expertise sind entscheidend, um im aufkommenden Quantenzeitalter wettbewerbsfähig zu bleiben und frühzeitig neue Wertschöpfungspotentiale zu erschließen.

2 Einführung in die Quantentechnologie

Beschleunigte technologische Durchbrüche, zunehmende Investitionsströme, die Verbreitung von Startups und Versprechen leistungsfähiger Quantensysteme bis 2030 signalisieren, dass es für Unternehmer und Investoren an der Zeit ist, ihre Strategien für Quantentechnologie zu planen.

Quantencomputer befinden sich zwar noch in der Experimentierphase, könnten jedoch künftig tiefgreifende Auswirkungen auf die Finanz- und Realwirtschaft haben.¹ Durch schnellere und potentiell effizientere Lösungen könnten Quantencomputer komplexe Probleme von höchster Relevanz bewältigen.



Quantencomputing ist der nächste technologische Durchbruch, der die Welt verändern wird.

Ginni Rometty, ehemalige CEO von IBM²



Quantum Computing hat das Potenzial, den Ursprung des Universums zu erklären.

Pfeiffer et al. (2021, Quantum Computing)



Ein **Quantencomputer** ist ein neuartiges Rechnersystem, das die Gesetze der Quantenmechanik nutzt, um bestimmte Berechnungen exponentiell schneller durchzuführen als klassische Computer. Im Gegensatz zu klassischen Computern, die mit Bits (0 oder 1) arbeiten, verwendet ein Quantencomputer Quantenbits (Qubits), die sich durch Überlagerungszustände und Verschränkung auszeichnen – dadurch können Qubits gleichzeitig mehrere Zustände annehmen und parallel verarbeiten. Diese einzigartigen Eigenschaften ermöglichen es Quantencomputern, komplexe Optimierungsprobleme zu lösen, die für klassische Computer praktisch unlösbar sind.

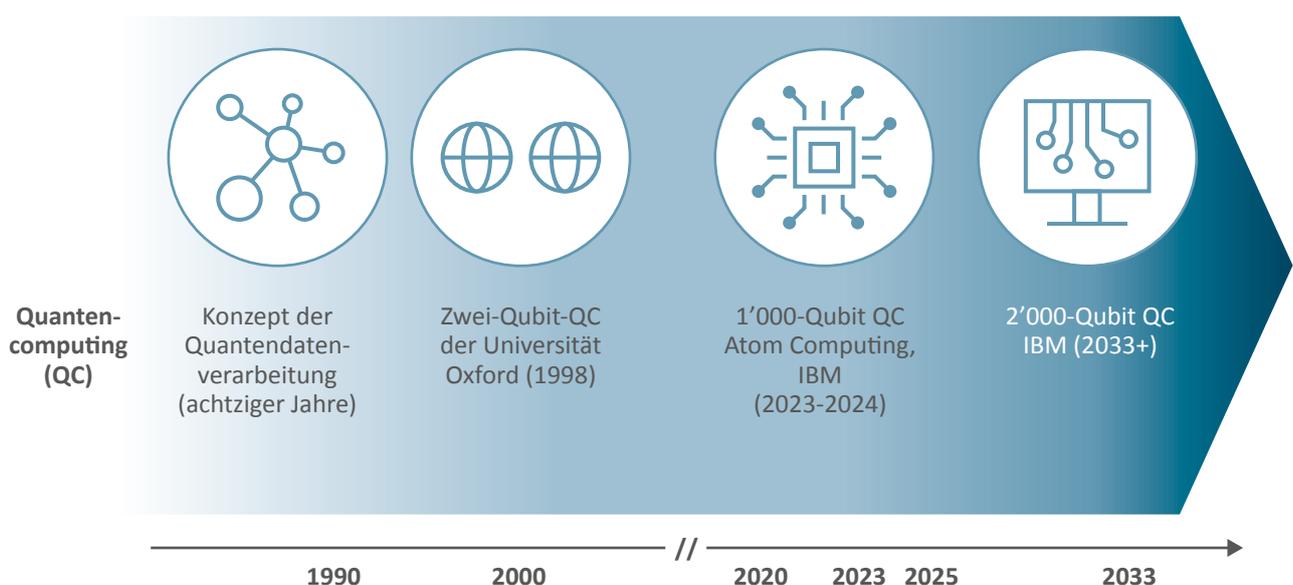
Qubits sind die grundlegenden Informationseinheiten eines Quantencomputers, vergleichbar mit den Bits in klassischen Computern. Anders als klassische Bits, die entweder den Zustand 0 oder 1 annehmen können, ermöglichen Qubits durch das quantenmechanische Prinzip der Superposition eine gleichzeitige Verarbeitung beider Zustände. Diese besonderen Eigenschaften werden in der Praxis durch verschiedene physikalische Systeme realisiert, etwa durch einzelne Atome, Elektronenspins oder supraleitende Schaltkreise. Während drei klassische Bits nur einen von acht möglichen Zuständen darstellen können, vermögen drei Qubits durch Superposition alle acht Zustände gleichzeitig zu verarbeiten.

Quantensimulationsalgorithmen lassen sich beispielsweise für Stresstests und makroökonomische Analysen nutzen, während Quantenoptimierung in der Vermögensbewertung Anwendung finden kann. Gleichzeitig stellt die Einführung von Quantencomputern eine potentielle Bedrohung für die Finanzstabilität dar, insbesondere durch ihre Fähigkeit, einige der am häufigsten verwendeten kryptografischen Algorithmen zu brechen. Trotz des frühen Entwicklungsstadiums der noch jungen Quantentechnologie erfordert allein die Möglichkeit, sensible Daten heute zu speichern, um sie später zu entschlüsseln, sofortige Vorbereitungen. Diese Abhandlung untersucht das transformative Potential der Quantenmechanik und ihre Anwendungen in der Finanz- und Realwirtschaft, einschließlich potentieller Vorteile und Hauptrisiken. Zudem werden aktuelle Maßnahmen von Anwenderunternehmen, Technologieentwicklern und Zentralbanken zur Bewältigung dieser potentiellen Risiken hervorgehoben.

Ein prominentes Beispiel für diese Maßnahmen ist das *Project Leap*³, initiiert von der *Bank für Internationalen Zahlungsausgleich (BIZ)* in Zusammenarbeit mit der *Banque de France* und der *Deutschen Bundesbank*. Das Projekt markiert einen entscheidenden Schritt zur Absicherung des globalen Finanzsystems gegen Quantencomputer-basierte Bedrohungen. Im Zentrum des Projekts steht die praktische Erprobung quantenresistenter Verschlüsselungsprotokolle im Zahlungsverkehr zwischen Zentralbanken. Besonders bemerkenswert ist der hybride Ansatz, bei dem klassische Verschlüsselungsverfahren mit zukunftssicheren, quantenresistenten Algorithmen kombiniert werden. Die erfolgreiche erste Projektphase hat bereits die technische Machbarkeit demonstriert, während die zweite Phase die Implementierung in komplexeren IT-Umgebungen unter Einbindung weiterer Zentralbanken vorsieht. Für Investoren ist dies ein wichtiges Signal, dass die Stabilität und Sicherheit der Finanzinfrastruktur auch angesichts der aufkommenden Quantentechnologie gewährleistet werden können.

In den letzten Jahren hat sich die Forschung und Entwicklung (F&E) im Bereich Quantencomputing beschleunigt. Nach der ursprünglichen Idee in den 1980er Jahren⁴ wurde das Konzept 1998 der Realität nähergebracht, als Forscher der *Universität Oxford* den ersten *Zwei-Qubit-Quantencomputer (QC)* entwickelten und damit das Potential der Quantenphysik für Berechnungen demonstrierten.⁵ Zwischen 2023 und 2024 erreichten experimentelle QCs eine Größe von 1'000 Qubits⁶, was einen bedeutenden Anstieg der Rechenleistung markierte. Stand 2024 befinden sich QCs zwar noch in der Experimentierphase, jedoch streben Technologieentwickler Systeme mit 2'000 logischen Qubits⁷ an, mit dem Ziel, die volle Leistungsfähigkeit des Quantencomputing ab 2033 bereitzustellen (Abb. 1).

Abb. 1: Entwicklung der Quantencomputertechnik im Laufe der Zeit



Quelle: Auer et al. (2024, Quantum im Finanzwesen)

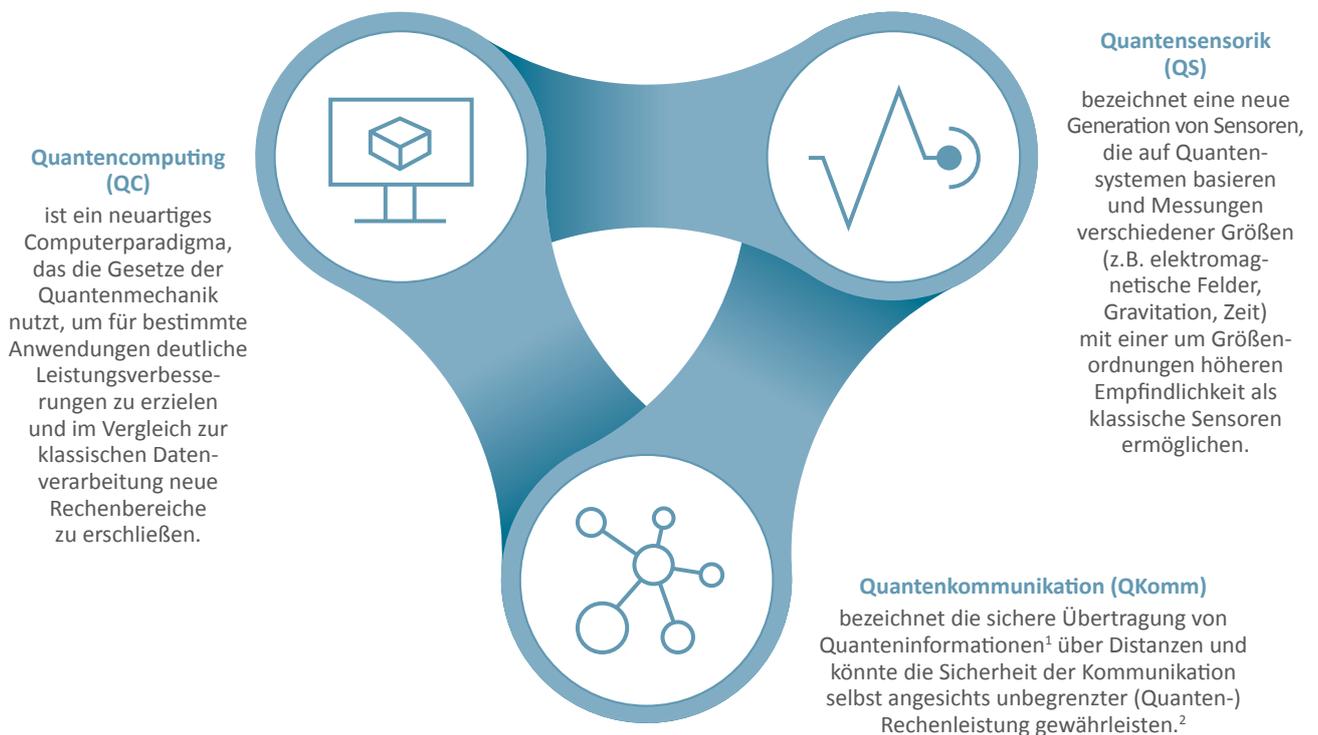
2.1 Definition und grundlegende Prinzipien der Quantentechnologie

Quantentechnologie ist ein Teilbereich der Informatik, der auf der Quantentheorie basiert. Sie ist eine hochmoderne Technologie, die Quantenmechanik nutzt, um schwierigere Probleme für klassische Computer zu lösen. Quantencomputer ermöglichen es, Konzepte aus der Quantenphysik im Computing zu nutzen. Sie unterscheiden sich von herkömmlichen Computern hinsichtlich Geschwindigkeit, Daten und Bits. Quantencomputer können genutzt werden, um genauere und produktivere maschinelle Lernberechnungen zu erstellen, die in Anwendungen wie Bild- und Spracherkennung eingesetzt werden.

Aktuell steht die Quantentechnologie an der Schwelle, verschiedene Wirtschaftszweige grundlegend zu transformieren. Diese zukunftsweisende Technologie umfasst drei zentrale Bereiche: Quantencomputing, Quantenkommunikation und Quantensensorik (vgl. Abb. 2).

Jeder dieser Bereiche verspricht Innovationen, die potentiell sowohl technologische als auch wirtschaftliche Paradigmen verschieben können.

Abb. 2: Computing, Kommunikation und Sensorik als Teilbereiche der Quantentechnologie



1. Quanteninformation unterscheidet sich von klassischer Information dadurch, dass die Information als Quantenzustände in Qubits gespeichert wird. Qubits sind die Informationseinheit für QC und eine Erweiterung des klassischen Bits (der Informationseinheit für klassische Computer).
2. Die Quantenkryptographie basiert auf dem Austausch eines geheimen Schlüssels zur Verschlüsselung von Nachrichten mittels des quantenmechanischen Phänomens der Verschränkung. Im Gegensatz zu klassischen kryptographischen Protokollen ist es nicht möglich, Nachrichten der Quantenkryptographie unbemerkt abzuhören. Allerdings haben sich bei frühen Implementierungen einige Schwachstellen gezeigt, die beispielsweise durch die physikalische Umsetzung der Protokolle verursacht wurden.

Quelle: Zimmel et al. (2024, Quantum-Monitor)

Quantencomputing (QC) stellt einen grundlegend neuen Ansatz der Datenverarbeitung dar. Anders als klassische Computer, die mit Bits (0 oder 1) arbeiten, verwenden Quantencomputer sogenannte *Qubits*, die sich gleichzeitig in mehreren Zuständen befinden können. Qubits nehmen also nicht nur die Zustände 0 und 1 an, sondern auch Überlagerungen (Superpositionen) dieser Zustände. Zudem können Qubits miteinander verschränkt sein.⁸ Diese quantenmechanischen Eigenschaften ermöglichen parallele Berechnungen und eine exponentielle Steigerung der Rechenleistung.⁹ Dies ermöglicht es, bestimmte komplexe Berechnungen erheblich schneller durchzuführen als mit herkömmlichen Computern. Die Technologie verspricht Durchbrüche in der Medikamentenentwicklung, Materialforschung und Finanzmodellierung. *McKinsey* prognostiziert für diesen Bereich bis 2035 ein Marktvolumen von 28 bis 72 Mrd. EUR.¹⁰

Quantenkommunikation (QKomm) konzentriert sich auf die abhörsichere Übertragung von Quanteninformation über große Distanzen. Im Gegensatz zu klassischen Verschlüsselungsmethoden, die von zukünftigen Quantencomputern möglicherweise geknackt werden könnten, bietet die Quantenkommunikation eine theoretisch nicht zu brechende Sicherheit. Diese basiert auf physikalischen Gesetzen statt auf mathematischer Komplexität. Die Technologie nutzt dabei quantenmechanische Effekte wie die Verschränkung. Laut *McKinsey* wird der Markt für Quantenkommunikation bis 2035 auf 11 bis 15 Mrd. EUR anwachsen, mit Anwendungen in der Absicherung kritischer Infrastruktur und im Finanzsektor.¹¹

Quantensensorik (QS) bezeichnet eine neue Generation hochempfindlicher Messgeräte, die quantenmechanische Effekte nutzen, um eine bisher unerreichte Präzision bei der Messung verschiedener physikalischer Größen zu erreichen. Diese Sensoren können elektromagnetische Felder, Schwerkraft und Zeit um Größenordnungen genauer messen als klassische Sensoren. Die Anwendungsmöglichkeiten reichen von der medizinischen Bildgebung über GPS-unabhängige Navigation bis hin zur unterirdischen Kartierung. *McKinsey* schätzt das Marktpotential bis 2035 auf 0,5 bis 2,7 Mrd. EUR.¹²

Der *McKinsey Quantum Technology Monitor* zeigt, dass sich diese drei Bereiche zwar unterschiedlich schnell entwickeln, aber alle wesentlichen Bestandteile des Quantentechnologie-Ökosystems sind. Gemeinsam könnten sie bis 2035 einen wirtschaftlichen Mehrwert von etwa 2 Bio. EUR schaffen, besonders in den Bereichen Chemie, Biowissenschaften, Finanzen und Mobilität. Der Bericht erfasst 367 Quantentechnologie-Startups weltweit (Stand 2024), mit kumulierten privaten und Unternehmens-Investitionen von 8,5 Mrd. EUR. Staaten weltweit haben bereits Förderungen von rund 42 Mrd. EUR für Quantentechnologien angekündigt.¹³

Diese Entwicklungen unterstreichen die strategische Bedeutung der Quantentechnologie für den Wirtschaftsstandort Deutschland und bieten erhebliche Chancen für zukunftsorientierte Investoren.

Bereits seit 2019 analysiert das FERI Cognitive Finance Institute die Entwicklungen im Bereich der Quantentechnologie, u.a. in den Publikationen „Quantencomputer, Internet of Things und superschnelle Kommunikationsnetze“, „The Great Progression“ sowie „KI: The Next Level“.



Die Quantenrevolution wird jeden Aspekt unseres Lebens beeinflussen, von der Gesundheitsversorgung bis zur Finanzwelt.

Chad Rigetti, Gründer von *Rigetti Computing*¹⁴



2.2 Vergleich mit klassischer Computertechnologie

Klassische Computer, wie wir sie seit Jahrzehnten kennen, verarbeiten Informationen in Form von Bits (0 oder 1) und führen Berechnungen nacheinander (seriell) aus. Bei komplexen Aufgaben, wie der Primfaktorzerlegung großer Zahlen oder der Simulation chemischer Reaktionen, stoßen sie trotz stetiger Leistungssteigerungen an fundamentale Grenzen. Ein klassischer Supercomputer würde beispielsweise Millionen von Jahren benötigen, um bestimmte kryptographische Codes zu knacken.

Quantencomputer hingegen nutzen die Gesetze der Quantenmechanik und können durch Quantenbits (Qubits) mehrere Zustände gleichzeitig verarbeiten. Dadurch sind sie in der Lage, spezifische Probleme exponentiell schneller zu lösen – was im konkreten Beispiel bedeutet, dass komplexe Berechnungen in Sekunden statt in Jahren durchgeführt werden können. Es wäre jedoch ein Missverständnis anzunehmen, dass Quantencomputer klassische Computer generell ersetzen werden. Sie sind nicht für alle Arten von Berechnungen überlegen, sondern nur für bestimmte, hochspezialisierte Aufgaben optimiert.



Quantencomputer werden uns helfen, Probleme zu lösen, die für klassische Computer unlösbar sind.

David Deutsch, Physiker an der *Universität Oxford*¹⁵



Die Zukunft liegt in der intelligenten Kombination beider Technologien in hybriden Systemen.¹⁶ Dabei übernehmen klassische Computer die Steuerung, Datenvorbereitung und Fehlerkorrektur, während Quantenprozessoren für rechenintensive Teilaufgaben in Bereichen wie Materialforschung, Finanzmodellierung oder Logistiko Optimierung eingesetzt werden. Diese Arbeitsteilung ermöglicht es Unternehmen, die jeweiligen Stärken beider Systeme optimal zu nutzen und neue Wertschöpfungspotentiale zu erschließen.

Während Quantencomputer oft als Zukunftstechnologie mit revolutionärem Potential gelten, wird der praktische Nutzen von Quantencomputern sich voraussichtlich auf wenige, aber wichtige Anwendungsgebiete beschränken.¹⁷

Konkrete Beispiele verdeutlichen dies: Bei alltäglichen Aufgaben wie Datenbankanfragen, Bildverarbeitung oder der Analyse von Geschäftsdaten bleiben klassische Computer überlegen. Ein Quantencomputer würde für diese Aufgaben sogar mehr Zeit benötigen. Der Grund: Der Overhead für die Quantenverarbeitung und Fehlerkorrektur übersteigt bei kleinen Datenmengen den theoretischen Geschwindigkeitsvorteil.

Echte Quantenvorteile entstehen erst bei sehr großen Datenmengen und/oder bei der

- Simulation komplexer Moleküle in der Pharmaforschung
- Optimierung globaler Logistiknetzwerke
- Analyse von Finanzmärkten in Echtzeit
- Entschlüsselung komplexer Verschlüsselungen



Quantencomputing wird uns helfen, die komplexesten Probleme der Welt zu lösen, von der Klimamodellierung bis zur Optimierung von Lieferketten.

Arvind Krishna, CEO von *IBM*¹⁸



Für Investoren bedeutet dies: Quantencomputing wird zwar kein universeller Ersatz für klassische Computer, aber ein unverzichtbares Werkzeug für spezifische Hochleistungsanwendungen. Die Technologie wird dort zum Einsatz kommen, wo klassische Computer an ihre Grenzen stoßen – typischerweise, wenn die Problemgröße 10^{12} übersteigt (Abb. 3, links). Ein konkretes Beispiel verdeutlicht die Größenordnung: Von einem „Quantenvorteil“ spricht man ab etwa einer Billion (10^{12}) Datenpunkten. Zum Vergleich:

- Eine typische Unternehmensdatenbank enthält 10^6 bis 10^9 Einträge.
- Das gesamte Internet umfasst etwa 10^{13} Webseiten.
- Die DNA eines Menschen besteht aus etwa 10^{10} Basenpaaren.¹⁹

Der wirtschaftliche Nutzen von Quantencomputern hängt stark vom konkreten Anwendungsfall ab, wobei vier Schlüsselsektoren bis 2035 ein Wertschöpfungspotential von bis zu 2 Bio. USD aufweisen.²⁰ Ein Beispiel aus der Finanzbranche verdeutlicht dies: Bei der Portfoliooptimierung mit 10^{12} Datenpunkten könnte ein Quantencomputer theoretisch in unter einer Sekunde die optimale Anlagestrategie berechnen – was klassische Computer etwa 100 bis 200 Stunden kostet.²¹ Allerdings relativiert sich dieser Geschwindigkeitsvorteil durch praktische Faktoren wie Marktschwankungen und ungenaue Prognosen.

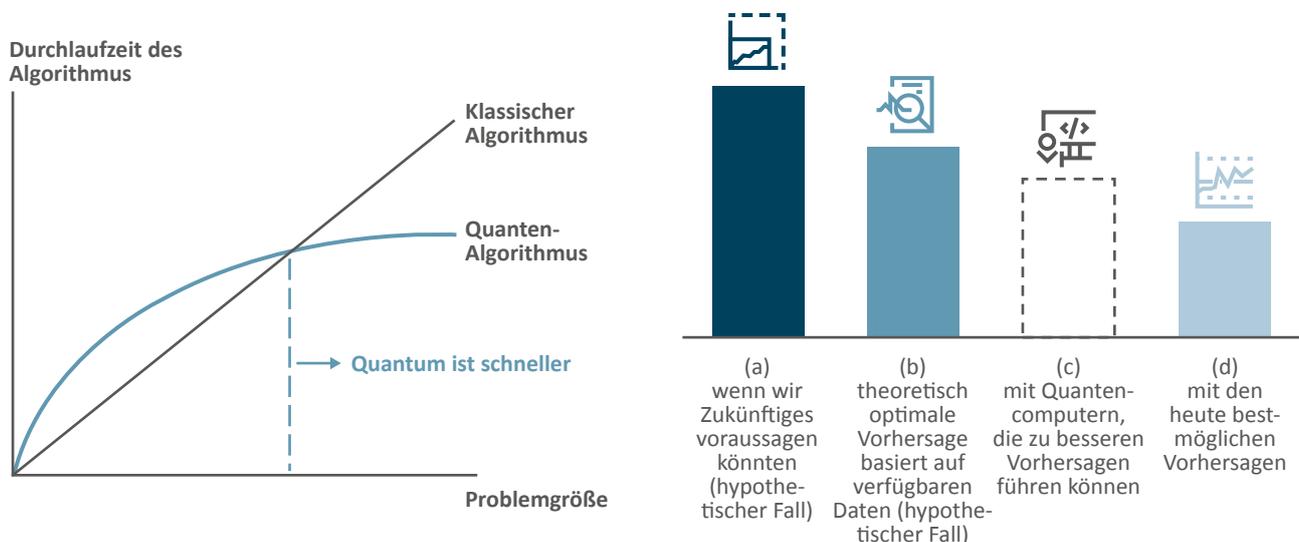
“
Mit Quantum Computing können wir
physikalische Bereiche untersuchen,
die uns sonst nicht zugänglich wären.
”

Pfeiffer et al. (2021, Quantum Computing)

Anders sieht es bei der Entwicklung neuer Materialien aus: Hier könnte die präzise Simulation von Molekülstrukturen durch Quantencomputer Entwicklungszeiten von durchschnittlich drei bis vier Jahren auf sechs bis acht Wochen verkürzen und damit Entwicklungskosten von typischerweise 2 bis 3 Mrd. USD pro Material um bis zu 25 % reduzieren.²² Ähnliches gilt für die Pharmaforschung, wo die exakte Berechnung von Proteinwechselwirkungen die Medikamentenentwicklung revolutionieren könnte. Hier liegt das Einsparpotential bei 500 Mio. bis 1 Mrd. USD pro Entwicklungszyklus.²³

Diese Beispiele zeigen: Der größte wirtschaftliche Mehrwert entsteht dort, wo Geschwindigkeit und Präzision direkt zu messbaren Wettbewerbsvorteilen führen – nicht bei Routineberechnungen oder in Bereichen mit hoher Datenunsicherheit. Diese Überlegungen gelten auch für den wirtschaftlichen Nutzen, der durch die Lösung derselben Probleme mit einem Quantencomputer erzielt werden kann (Abb. 3, rechts).

Abb. 3: Auswirkungen der Quanteninformatik



Quelle: Auer et al. (2024, Quantum im Finanzwesen)

2.3 Potentielle Anwendungen und Vorteile der Quantentechnologie

Quantencomputer versprechen Durchbrüche in vielen Bereichen wie Logistik, Luft- und Raumfahrt sowie Schifffahrt, Finanzwesen, Chemie, Pharmazie und Materialwissenschaften.²⁴ In der Logistik könnten sie Probleme wie die Optimierung von Lieferketten und Tourenplanung effizienter lösen, im Bereich der Luft- und Schifffahrt lassen sich insbesondere Wartungsprozesse, Routen sowie Zuordnungen von Gates bzw. Kais optimieren. Banken und Versicherungen erhoffen sich besseres Risikomanagement, genauere Modelle und schnellere Transaktionen. In Chemie und Pharmazie verspricht Quantencomputing genauere Simulationen von Molekülen für die Medikamentenentwicklung. Zudem könnten neuartige Hochleistungswerkstoffe entwickelt werden. Langfristig könnte durch Implementierung von Künstlicher Intelligenz auf Quantencomputern sogar Generelle Künstliche Intelligenz (AGI) möglich werden.

Generelle Künstliche Intelligenz (Artificial General Intelligence; AGI) bezeichnet das bislang noch theoretische Prinzip einer maschinenbasierten Intelligenz, die in allen wesentlichen Belangen dem menschlichen Intellekt und Denkvermögen mindestens gleichwertig oder überlegen ist.

Die Grundlagen sowie das theoretische Prinzip hinter der Entwicklung einer Generellen Künstlichen Intelligenz (AGI) wurden vom FERI Institut bereits 2023 ausführlich erörtert in der Analyse „**KI: The Next Level: Die transformative Wucht des Megatrends Künstliche Intelligenz**“.



Wie Quantencomputer in Zukunft die Biotechnologie verändern, analysierte das FERI Institut gemeinsam mit Bio^M in der Studie „**Die BioTech-Revolution**“.

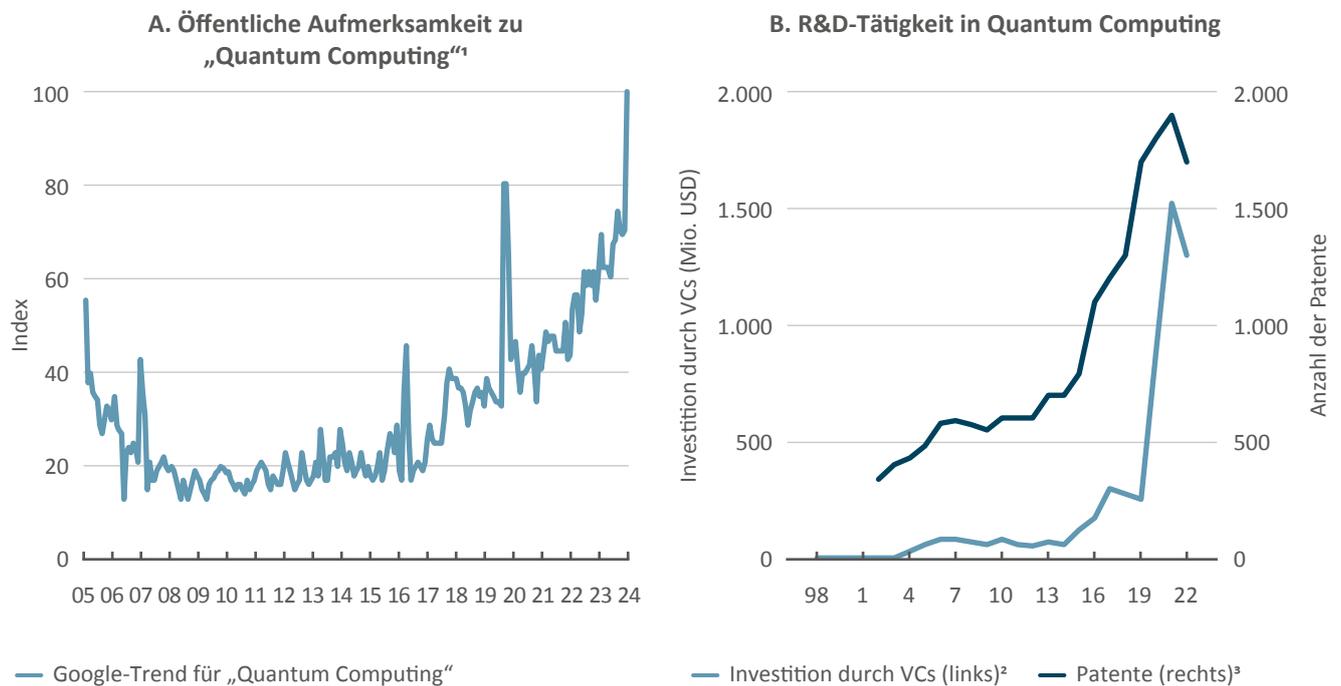


2.4 Adaptionszyklus

Dieses Potential und die rasante Entwicklung in diesem Bereich haben die Aufmerksamkeit aller relevanten Akteure auf sich gezogen: Forscher, Investoren, Finanzmarktakteure und politische Entscheidungsträger (Abb. 4.A). Das wachsende Interesse an den neuen Möglichkeiten, die Quantencomputer bieten, führt zu einer wechselseitigen Interaktion zwischen steigenden Investitionen von Risikokapitalgebern in Projekte im Bereich des Quantencomputing und neuen Entdeckungen in diesem Forschungsgebiet (Abb. 4.B).

Das Finanzsystem ist durch komplexe Berechnungen für Analysen, Prognosen und Optimierungen gekennzeichnet. Angesichts der hohen Dimensionalität der zugrunde liegenden Probleme stoßen die heutigen Hochleistungscomputer oft an ihre Grenzen, wenn es um die rechnerische Komplexität dieser Aufgaben geht. Quantencomputing mit seiner potentiellen Fähigkeit, riesige Mengen an Lösungszuständen zu verarbeiten und komplexe Berechnungen effizient durchzuführen, verspricht, einige dieser Herausforderungen zu bewältigen. Tatsächlich wird prognostiziert, dass die Finanzbranche eine der ersten Branchen sein dürfte, die von Quantencomputing profitieren wird.

Abb. 4: Zunehmende Aufmerksamkeit und FuE-Aktivitäten im Bereich Quantencomputer



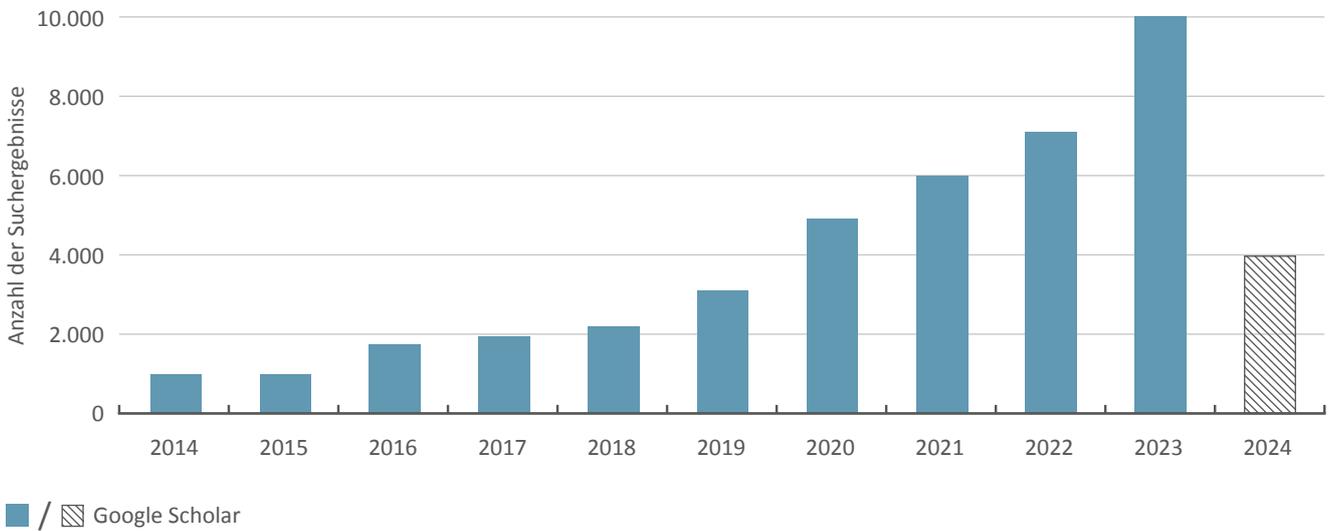
1. Google-Tendenzindex für „Quantum Computing“ per 15. Dezember 2023.
2. Investition durch VCs zeigt den Gesamtwert an, der von den Risikokapitalgebern in den Unternehmen investiert wurde, die in Quantum Computing-Projekte involviert sind.
3. Die Anzahl der Patente basiert auf Patenten, die „Quantum“ in ihrem Abstract enthalten und die von US- oder EU-Patentämtern ausgegeben wurden.

Quelle: Auer et al. (2024, Quantum im Finanzwesen)

Das Interesse an Anwendungen im Finanzbereich nimmt daher zu, was sich auch in der steigenden Anzahl von Publikationen in diesem Bereich widerspiegelt (Abb. 5). Bei wissenschaftlichen Veröffentlichungen zum Quantencomputing liegt China knapp vorn. Eine Analyse von 2023 ergab, dass europäische Forscher etwa 24 % der Publikationen zum Quantencomputing verantworten, gefolgt von China mit 23 % und den USA mit 17 %.²⁵ Die Qualität und Zitierhäufigkeit der US-Publikationen ist jedoch im Durchschnitt höher, was auf eine möglicherweise größere Innovationskraft hindeutet.

Auf die Frage „Wie verhält sich das Entwicklungstempo im Vergleich zu Ihren Erwartungen von vor einigen Jahren?“ gaben über 50 % der Befragten an, dass das Entwicklungstempo schneller (41,2 %) oder viel schneller (10,2 %) ist, als sie erwartet hatten (Abb. 6).²⁶ Dies geht aus einer aktuellen Umfrage von *QuEra Computing* vom Juni 2024 hervor. Die Studie liefert wichtige Erkenntnisse zu nationalen Quantenprogrammen, technischen Herausforderungen, Entwicklungsgeschwindigkeit und ethischen Überlegungen im Bereich des Quantencomputing. Von den 927 Teilnehmern, die zwischen Mitte Juni und Anfang Juli 2024 befragt wurden, kam der größte Anteil aus dem akademischen Bereich, gefolgt von Quantencomputing-Unternehmen und branchenfremden Firmen. Auch Enthusiasten, Analysten und andere Interessengruppen wie gemeinnützige Forscher, Berater und Studierende waren unter den Befragten vertreten.

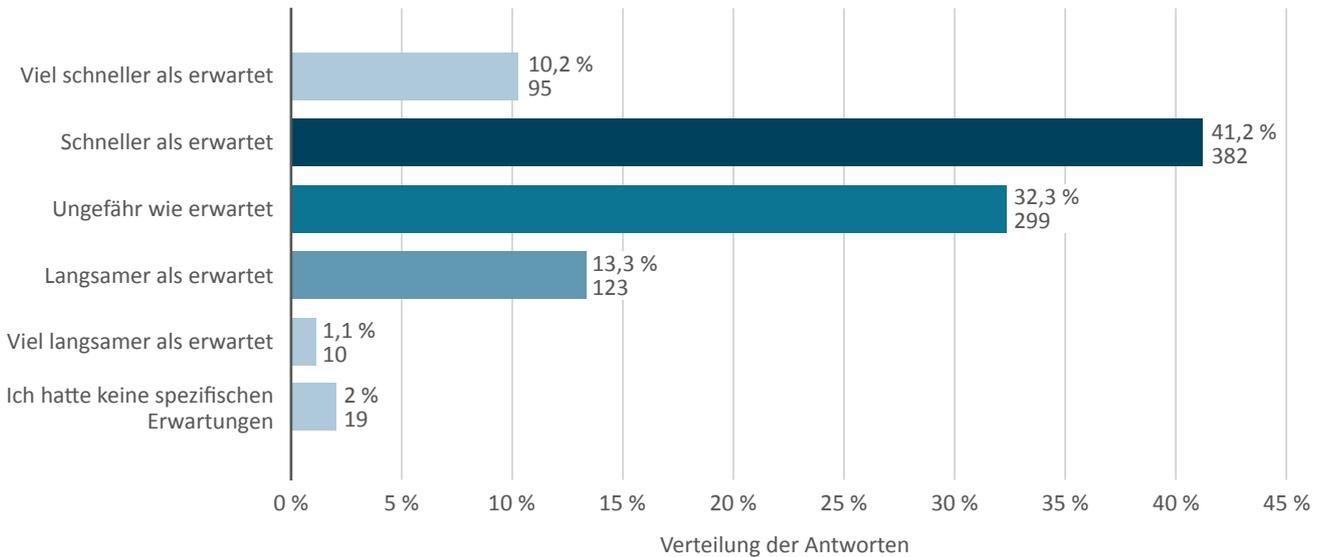
Abb. 5: Quantencomputer und Finanzen: Google Scholar Ergebnisse



Hinweis: Die y-Achse repräsentiert die Anzahl der Suchergebnisse, die von *Google Scholar* abgerufen wurden (quantifiziert in absoluten Zahlen). Jeder Datenpunkt entspricht der Gesamtanzahl der Einträge (z.B. Artikel, Papiere, Dissertationen), die von *Google Scholar* für eine bestimmte Suchanfrage zurückgegeben wurden. Die x-Achse zeigt die spezifischen untersuchten Zeiträume, wobei jeder entsprechende Punkt die kumulative Anzahl der indizierten Ergebnisse widerspiegelt. Für 2024 wurden Daten bis zum 19. Juni 2024 verwendet.

Quelle: Auer et al. (2024, Quantum im Finanzwesen)

Abb. 6: Tempo der Entwicklung im Vergleich zu den individuellen Erwartungen



Quelle: QuEra Computing (2024, Umfrage)

3 Quantentechnologie

3.1 Quantenbits (Qubits) und ihre Eigenschaften

Qubits (Quantenbits) sind die fundamentalen Informationseinheiten in Quantencomputern (QCs), vergleichbar mit Bits in klassischen Computern.²⁷ Sie basieren auf quantenmechanischen Zwei-Zustands-Systemen, wie dem Spin eines Elektrons oder den Energieniveaus eines Atoms.²⁸ Im Gegensatz zu klassischen Bits, die entweder 0 oder 1 sind, können Qubits in einer **Überlagerung** (Superposition) dieser Zustände existieren (Abb. 7).

Abb. 7: Quantenbits (Qubits)



Quelle: Hussain/Talib (2016, Quantum-Diskussion)

Um dies zu veranschaulichen, hilft der Vergleich mit einer Münze, die nicht nur „Kopf“ oder „Zahl“ sein kann, sondern auch auf der Kante balanciert – in einem Zustand zwischen beiden Möglichkeiten. Diese Superposition erlaubt es einem einzelnen Qubit, eine Kombination von zwei Zuständen darzustellen, was die Informationsdichte exponentiell erhöht.²⁹

Eine weitere faszinierende Eigenschaft von Qubits ist die **Verschränkung**. Verschränkte Qubits teilen einen gemeinsamen Quantenzustand, unabhängig von ihrer räumlichen Trennung. Dies lässt sich mit zwei perfekt synchronisierten Tänzern vergleichen, die ihre Bewegungen sofort aufeinander abstimmen, ohne sichtbare Kommunikation.

Die Kombination aus Superposition und Verschränkung eröffnet völlig neue Möglichkeiten für Berechnungen. Ein 1'000-Qubit-QC kann theoretisch $2^{1'000}$ verschiedene Zustände gleichzeitig repräsentieren – eine Zahl, die die Anzahl der Atome im beobachtbaren Universum bei weitem übersteigt.³¹

Diese einzigartigen Eigenschaften ermöglichen es QCs, bestimmte komplexe Probleme wesentlich effizienter zu lösen als klassische Computer. Beispielsweise könnte die Optimierung von Handelsstrategien oder die Simulation ganzer Finanzmärkte, die auf klassischen Computern Jahre dauern würde, auf QCs in Stunden oder Minuten durchgeführt werden.³²

“
Quantencomputer sind der Schlüssel zur Entschlüsselung der Geheimnisse des Universums.

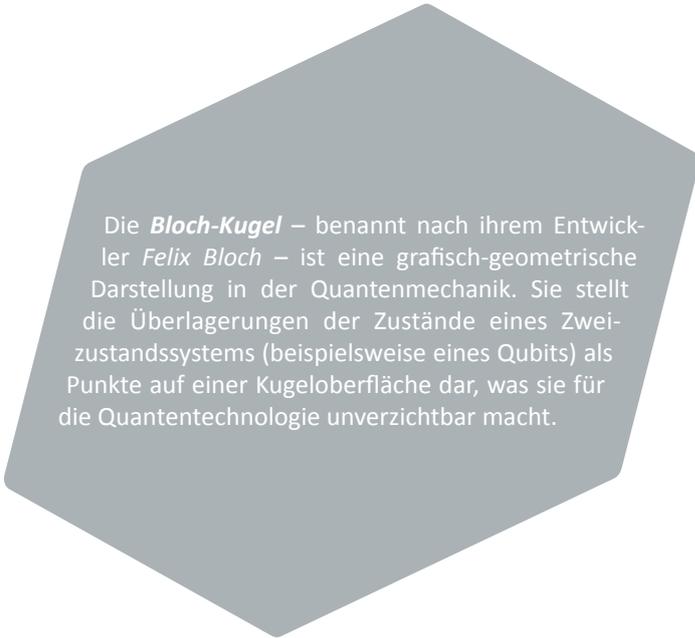
Seth Lloyd, Professor für Maschinenbau am MIT³⁰

“

Allerdings stehen QCs vor erheblichen Herausforderungen. Qubits sind äußerst empfindlich gegenüber Umwelteinflüssen und erfordern aufwendige Isolierung und Kühlung auf nahezu den absoluten Nullpunkt. Diese Störanfälligkeit, bekannt als *Dekohärenz*, begrenzt derzeit die praktische Anwendbarkeit von QCs.³³

3.2 Quantengatter und Operationen

Berechnungen auf Quantencomputern werden durch *Quantengatter* realisiert. Diese führen Operationen auf einem oder mehreren Qubits aus und erzeugen verschränkte Zustände. Wichtige Ein-Qubit-Gatter sind die *Hadamard-Transformation*, die Qubits in Superposition versetzt, und die *Pauli-Gatter*, die Drehungen um die X-, Y- und Z-Achse der *Bloch-Kugel* durchführen.³⁴ Zu den wichtigsten Zwei-Qubit-Gattern zählen das *Controlled-NOT (CNOT)* und das *Controlled-Z (CZ)*, die ein Qubit in Abhängigkeit vom Zustand eines Kontrollqubits invertieren, also umkehren. Aus diesen elementaren Gattern lassen sich komplexere Schaltungen aufbauen.



Die *Bloch-Kugel* – benannt nach ihrem Entwickler *Felix Bloch* – ist eine grafisch-geometrische Darstellung in der Quantenmechanik. Sie stellt die Überlagerungen der Zustände eines Zweizustandssystems (beispielsweise eines Qubits) als Punkte auf einer Kugeloberfläche dar, was sie für die Quantentechnologie unverzichtbar macht.

3.3 Quantenalgorithmen und Protokolle

Quantenalgorithmen nutzen die speziellen Eigenschaften von Qubits für eine effiziente Lösung bestimmter Probleme.³⁵ Der bekannteste ist der *Shor-Algorithmus* zur Primfaktorzerlegung, der eine exponentielle Beschleunigung gegenüber klassischen Methoden verspricht und die Sicherheit heutiger Verschlüsselung bedroht. Der *Grover-Algorithmus* ermöglicht eine quadratische Beschleunigung für die Suche in unstrukturierten Datenbanken. Weitere wichtige Algorithmen sind die *Quanten-Fouriertransformation* für die Spektralzerlegung periodischer Funktionen und das *Quanten-Phasenschätzungsprotokoll*, das viele Anwendungen besitzt.

In Zukunft werden Quantenalgorithmen die Künstliche Intelligenz revolutionieren, indem sie die Verarbeitungskapazität von KI-Systemen exponentiell steigern: Während das aktuelle GPT-4 mit seinen 175 Milliarden Parametern für eine präzise Übersetzung eines 1.000-Wörter-Textes etwa zwei bis drei Sekunden benötigt, könnte ein quantenbasiertes Sprachmodell mit 1 Billion Parametern den gleichen Text in Millisekunden übersetzen und dabei auch komplexe kulturelle Nuancen erfassen. Die Trainingszeit für solche Modelle würde sich dramatisch verkürzen – von derzeit sechs bis acht Monaten und Energiekosten von etwa 10 bis 15 Mio. EUR pro Training auf wenige Tage bei einem Bruchteil des Energieverbrauchs.³⁶ Konkret bedeutet das für Unternehmen: Ein KI-Assistent auf Quantenbasis könnte beispielsweise die gesamte Kommunikation eines multinationalen Konzerns in Echtzeit übersetzen, juristische Dokumente in Sekundenschnelle analysieren und gleichzeitig aus Millionen von Kundengesprächen präzise Geschäftsprognosen erstellen – Aufgaben, für die heute noch verschiedene spezialisierte Systeme mit jeweils eigenen Verzögerungszeiten nötig sind.

3.4 Quantenfehlerkorrektur und Fehlertoleranz

Qubits sind sehr empfindlich gegenüber Störungen aus der Umgebung. Schon geringste Wechselwirkungen können sie aus ihrer Superposition oder Verschränkung reißen, sodass Fehler entstehen. Die Quantenfehlerkorrektur kodiert logische Qubits in verschränkten Zuständen mehrerer physischer Qubits und nutzt Redundanz, um Fehler zu erkennen und zu korrigieren.³⁷ Bekannte Verfahren sind der *Shor-Code*, die *Oberflächencodes* und der *Farbcode*. Um fehlertolerantes Quantencomputing zu ermöglichen, darf die Fehlerrate der physischen Qubits und Gatter nicht über einem Schwellenwert liegen. Die Entwicklung skalierbarer und robuster Fehlerschutzarchitekturen ist deshalb eine der größten Herausforderungen für Quantencomputer.

4 Aktueller Stand der Quantentechnologie

4.1 Überblick über bestehende Plattformen für Quantentechnologie

Es gibt verschiedene physikalische Ansätze zur Realisierung von Quantencomputern. Am weitesten entwickelt sind supraleitende Qubits, bei denen die Zustände durch Stromkreise aus *Josephson-Kontakten* kodiert werden. *Google, IBM, Intel* und *Rigetti* verfolgen diesen Ansatz. Eine andere Plattform sind gefangene Ionen, bei denen Atome in einer *Paul-Falle* durch Laser manipuliert werden (vgl. dazu nachfolgende Erklärboxen). Führend ist hier *IonQ*. Weitere Ansätze sind *Spin-Qubits* in Quantenpunkten und Defekten in Diamant, kalte Atome in optischen Gittern, Photonen in integrierten Schaltkreisen und topologische Qubits wie *Majorana-Fermionen*. China verfolgt Quantencomputing auf Basis von Phosphor-Dotierungen in Silizium.

Josephson-Kontakte sind die zentralen Bauelemente in supraleitenden Quantencomputern und bestehen aus zwei supraleitenden Materialien, die durch eine hauchdünne isolierende Schicht getrennt sind. Diese speziellen elektronischen Bauelemente nutzen den quantenmechanischen Tunneleffekt, bei dem Elektronenpaare die isolierende Barriere durchqueren können, was zur Erzeugung und Steuerung von Qubits genutzt wird. Josephson-Kontakte sind besonders interessant für die praktische Umsetzung von Quantencomputern, da sie sich verhältnismäßig einfach in bestehende Halbleitertechnologien integrieren lassen und bei Temperaturen nahe dem absoluten Nullpunkt sehr präzise arbeiten.

Eine **Paul-Falle** ist ein hochpräzises physikalisches Instrument zur Speicherung einzelner geladener Teilchen mittels elektrischer Wechselfelder, benannt nach dem deutschen Physiker *Wolfgang Paul*. Die Technologie nutzt oszillierende elektrische Felder, um einzelne Ionen in einem definierten Bereich im freien Raum zu fixieren und zu manipulieren, wodurch diese als Qubits für Quantencomputer verwendet werden können. Diese Technologie zeichnet sich durch besonders lange Kohärenzzeiten aus, was bedeutet, dass die gespeicherte Quanteninformation über vergleichsweise lange Zeit stabil bleibt. Der Technologiekonzern *Honeywell* setzt in seinen Quantencomputern erfolgreich auf **Paul-Fallen** und erreicht damit Quantenoperationen mit einer Präzision von über 99,99 %.

4.2 Herausforderungen und Einschränkungen in der Quantentechnologie

Eine große Herausforderung ist die Skalierung auf eine hohe Anzahl an Qubits bei gleichzeitiger Verbesserung ihrer Kohärenz und Gattergenauigkeit.³⁸ Mit heutigen Technologien ist die Fehlerrate noch zu hoch für viele praktische Anwendungen. Auch die Erstellung komplexer Quantenschaltungen und deren Ansteuerung und Auslese ist aufwendig. Die Chips müssen nahe dem absoluten Nullpunkt betrieben werden, was hohe Anforderungen an die Kühlung stellt. Zudem ist eine effektive Schnittstelle zu klassischen Computern und eine Integration in hybride Systeme nötig. Weitere Herausforderungen betreffen Programmiersprachen, Compiler, Betriebssysteme und das Auffinden geeigneter Algorithmen und Anwendungsfälle.³⁹

4.3 Aktuelle Fortschritte und Durchbrüche auf dem Gebiet

In den letzten Jahren gab es im Bereich des Quantencomputing beeindruckende Fortschritte. So demonstrierte *Google* 2019 erstmals „Quantenüberlegenheit“⁴⁰ mit einem 54-Qubit-Prozessor namens *Sycamore*, der eine spezielle Testaufgabe in 200 Sekunden löste, wofür *IBMs* stärkster Supercomputer 10.000 Jahre bräuchte. 2020 präsentierte *IonQ* einen Quantencomputer mit 32 Ionen-Qubits und einer sehr geringen Fehlerrate. *Honeywell* und *CQC* arbeiten an Quantencomputern mit Ionenfallen. Ein Startup namens *PsiQuantum* will mittels Photonen-Qubits auf konventionellen Mikrochips in wenigen Jahren Systeme mit einer Million Qubits realisieren.⁴¹ Jüngst präsentierte *IBM* den „Osprey“-Prozessor mit 433 Qubits und will bis 2023 4'000 Qubits erreichen. Auch China vermeldet große Fortschritte.

Insbesondere im Jahr 2024 gab es bedeutende Fortschritte in der Quantencomputer-Forschung (siehe Tab. 1). Diese Entwicklungen zeigen, dass sich die Quantentechnologie rasch weiterentwickelt. Der Fokus liegt dabei nicht mehr nur auf der Erhöhung der Qubit-Anzahl, sondern zunehmend auf der Verbesserung der Zuverlässigkeit und Fehlertoleranz.

Tab. 1: Ausgewählte Durchbrüche im Quantencomputing

Organisation	Erklärung des Durchbruchs	Einordnung
Google	Quantencomputer <i>Sycamore</i> mit 70 Qubits demonstriert „Quantenüberlegenheit“ bei spezifischen Berechnungen	<i>Sycamore</i> kann bestimmte Berechnungen in Minuten durchführen, für die herkömmliche Supercomputer Tausende von Jahren benötigen würden. <i>Google</i> fokussiert sich darauf, Optimierungsprobleme zu lösen.
Quantinuum	56-Qubit-Ionenfallen-Quantencomputer erreichte Rekord-Zuverlässigkeit von 35 % bei Quantenüberlegenheits-Benchmark	Der H2-1-Quantenrechner löste den <i>Random Circuit Sampling Algorithmus (RCS)</i> mit deutlich geringerer Fehlerquote als bisherige Ansätze. Er benötigte 30.000-mal weniger Energie als ein Supercomputer für die gleiche Aufgabe.
Oxford Ionics	Neuer Quantenchip mit Ionen-Qubits erreicht Rekordpräzision bei Ein- und Zwei-Qubit-Gattern (99,9992 % bzw. 99,97 % Zuverlässigkeit)	Der Chip basiert auf gefangenen Ionen und soll in industriellem Maßstab in Halbleiterfabriken hergestellt werden können. Die gesamte Elektronik zur Kontrolle der Ionen ist auf einem Siliziumchip integriert, ohne Laser.
Universität zu Köln	Erzeugung supraleitender Effekte mit Stromfluss nur an den Außenkanten in speziellen Materialien, wichtiger Schritt für topologische Supraleitung und robuste Qubit-Kodierung	Die Forscher verwendeten dünne Schichten eines anomalen Quanten-Hall-Isolators mit einer supraleitenden Niob-Elektrode. Dies ermöglicht die Erzeugung chiraler Majorana-Zustände, die für topologisch geschützte „fliegende Qubits“ entscheidend sind. Majorana-Zustände sind spezielle quantenmechanische Teilchenzustände, die sich nur in eine Richtung an den Rändern topologischer Materialien ausbreiten und als ihre eigenen Antiteilchen fungieren.

Quelle: Blaschke (2024, Quantencomputing)

Google steigerte die Prozessorleistung seines *Sycamore* auf 70-Qubits⁴². Dies demonstriert eindrucksvoll das Potential von Quantencomputern, komplexe Berechnungen zu beschleunigen. Dies könnte in Zukunft sehr grundlegende Durchbrüche in Bereichen wie Materialforschung, Medikamentenentwicklung oder Finanzmodellierung ermöglichen.

Sycamore markiert einen bedeutenden Meilenstein in der Quanteninformatik. Der Prozessor erreichte die sogenannte „*Weak Noise Phase*“, in der die Berechnungsleistung diejenige der leistungsstärksten klassischen Supercomputer übertrifft. Diese Entwicklung wurde im Oktober 2024 in der renommierten Fachzeitschrift *Nature* veröffentlicht.⁴³ Der Quantenchip konnte durch die Reduzierung von Umgebungsrauschen auf ein Minimum – insbesondere durch den Betrieb bei nahezu absolutem Temperatur-Nullpunkt – die Fehlerquote von 99,4 % auf 99,7 % verbessern.⁴⁴ Diese scheinbar geringe Verbesserung führte zu einem bemerkenswerten Leistungssprung: Der Quantenprozessor übertraf erstmals klassische Hochleistungsrechner bei der Durchführung von *Random Circuit Sampling (RCS)*, also Quantenzufallsschaltungen.

Einblicke in das **Quantinuum System Model H2** gibt dieses Video.



Das Unternehmen *Quantinuum* erreichte mit seinem 56-Qubit-Ionenfallen-Quantencomputer eine Rekord-Zuverlässigkeit von 35 % bei einem Quantenüberlegenheits-Benchmark.⁴⁵ Während *Googles Sycamore*-Prozessor durch die Reduzierung des Umgebungsrauschens seine Fehlerquote auf 99,7 % verbessern konnte, erreichte der neue

56-Qubit-Ionencomputer von *Quantinuum* einen noch bedeutsameren Meilenstein: Bei der *Random Circuit Sampling (RCS)*-Aufgabe erzielte er eine XEB-Zuverlässigkeitsquote von 35 % – im Vergleich zu lediglich 0,2 % bei *Googles Sycamore* im Jahr 2019. Besonders bemerkenswert ist dabei der deutlich geringere Energieverbrauch des *Quantinuum*-Systems, das 30.000-mal weniger Energie als klassische Supercomputer benötigt. Diese Entwicklung signalisiert einen Paradigmenwechsel in der Quantencomputer-Architektur – weg von der reinen Maximierung der Qubit-Anzahl, hin zu fehlertoleranten Systemen. Für Anleger eröffnet dies neue Perspektiven, insbesondere im Hinblick auf Investitionen in Unternehmen, die sich auf die Optimierung der Quantenarchitektur spezialisiert haben.

Oxford Ionics entwickelte einen Quantenchip mit Ionen-Qubits, der eine Rekordpräzision erreicht.⁴⁶ Der neue Quantenchip des Unternehmens, der ohne Laser auskommt und stattdessen auf integrierte Elektronik setzt, demonstrierte mit bis zu zehn Qubits eine Rekordpräzision: 99,9992 % bei Ein-Qubit-Gattern und 99,97 % bei Zwei-Qubit-Gattern – ohne Fehlerkorrektur. Diese Leistung verdoppelt die bisher beste Performance im Bereich der Ionenfallen-Quantencomputer. Besonders bemerkenswert ist der industrielle Fertigungsansatz in Kooperation mit *Infineon* in Villach, der die Massenproduktion in Halbleiterfabriken ermöglichen soll. Das 2019 gegründete Unternehmen, das bereits 37 Mio. Pfund an Investitionen eingeworben hat, plant als nächsten Schritt die Entwicklung eines skalierbaren 256-Qubit-Chips. Die Erfolge von *Quantinuum* und *Oxford Ionics* bei der Verbesserung der Qubit-Kontrolle und -Zuverlässigkeit sind ebenfalls vielversprechend. Je präziser Quantengatter ausgeführt werden können, desto komplexere Quantenalgorithmen lassen sich implementieren.

An der *Universität zu Köln* gelang es Forschern, einen wichtigen Schritt für robustere Quantencomputer zu machen.⁴⁷ Das Team um *Yoichi Ando* konnte in speziellen Materialien supraleitende Effekte erzeugen, bei denen der Strom ausschließlich an den Außenkanten fließt. Durch die Kombination eines anomalen *Quanten-Hall-Isolators* mit einer supraleitenden Niob-Elektrode gelang es, die sogenannte gekreuzte *Andreev-Reflexion* nachzuweisen. Diese Entwicklung ist besonders relevant für die Erzeugung von *Majorana-Fermionen* und topologisch geschützten „fliegenden Qubits“. Das Projekt, das in Zusammenarbeit mit der *KU Leuven*, der *Universität Basel* und dem *Forschungszentrum Jülich* im Rahmen des Exzellenzclusters *ML4Q* durchgeführt wurde, könnte den Weg zu stabileren und effizienteren Quantencomputern ebnen, die weniger anfällig für Dekohärenz und Informationsverlust sind. Diese Forschung zu topologischen Supraleitern könnte besonders robuste Qubits hervorbringen. Dies wäre ein wichtiger Schritt in Richtung fehlertoleranter Quantencomputer.

Die Firma *Trumpf* hat einen bedeutenden Fortschritt in der Entwicklung industrietauglicher Quantencomputer erzielt.⁴⁸ In Zusammenarbeit mit der *Universität Stuttgart* und dem *Fraunhofer-Institut für Angewandte Festkörperphysik IAF* wurde ein Quantenprozessor entwickelt, der bei Raumtemperatur funktioniert. Dies stellt einen entscheidenden Schritt zur Praxistauglichkeit dar, da bisherige Quantencomputer aufwendige Kühlsysteme benötigen. Der neue Prozessor basiert auf Diamanten mit künstlich erzeugten Fehlstellen, sogenannten *Stickstoff-Fehlstellen-Zentren*, die als Qubits fungieren. Diese Innovation könnte die Anwendung von Quantencomputern in verschiedenen industriellen Bereichen, wie der Entwicklung neuer Materialien oder der Optimierung von Fertigungsprozessen, erheblich vorantreiben.

Ein weiterer bahnbrechender Fortschritt in der Quantenforschung wurde am 31. Oktober 2024 von Forschenden der *Empa* und deren internationalen Partnern erzielt.⁴⁹ Das Kernelement des Durchbruchs besteht in der exakten synthetischen Nachbildung des *Heisenberg-Modells* mittels einer kontrollierten Anordnung von Elektronenspins. Die *Empa*-Forschenden nutzten dafür das *Clar's Goblet* – ein spezielles Nanographen-Molekül aus elf Kohlenstoffringen in Sanduhrform, das an beiden Enden je ein ungepaartes Elektron mit entsprechendem Spin aufweist. Das methodische Novum liegt in der gezielten Verknüpfung dieser *Goblet*-Strukturen auf einer Goldoberfläche zu präzisen konfigurierbaren Ketten. Dabei gelang es erstmals, zwei unterschiedliche Kopplungsstärken zwischen den Spins zu realisieren: Eine schwache Kopplung innerhalb des Moleküls und eine starke Kopplung zwischen benachbarten Molekülen. Diese alternierende Anordnung entspricht exakt dem theoretischen *Heisenberg-Modell*. Die besondere Bedeutung dieser Entwicklung ergibt sich aus der nun möglichen experimentellen Überprüfbarkeit quantenphysikalischer Modelle. Die Forschenden können einzelne Spins gezielt manipulieren, deren Wechselwirkungen messen und die Kettenlänge präzise steuern. Diese Kontrolle über Quantenzustände ist fundamental für die Entwicklung *skalierbarer* Quantencomputer.

Trotz dieser Fortschritte stehen noch große Herausforderungen bevor. Die **Skalierung** auf Hunderte oder Tausende fehlerkorrigierte Qubits, die für praktisch relevante Anwendungen nötig sind, erfordert weitere Durchbrüche. Auch die Entwicklung von Quantenalgorithmen für reale Probleme steht noch am Anfang. Insgesamt zeigen die jüngsten Entwicklungen jedoch, dass das Feld der Quanteninformatik hochdynamisch ist. In den kommenden Jahren dürften weitere spannende Fortschritte zu erwarten sein, die das Potential haben, die Computertechnologie zu revolutionieren.

5 Quantentechnologie in der Praxis

5.1 Anwendungsfälle und praktische Anwendungen von Quantentechnologie

Die Quantentechnologie steht an der Schwelle zu praktischen Anwendungen und markiert damit den Beginn einer **neuen technologischen Ära**.

Pioniere wie *Volkswagen* nutzen bereits Quantenalgorithmen zur Verkehrsflussoptimierung und konnten die Rechenzeit für komplexe Routingprobleme von mehreren Wochen auf wenige Minuten reduzieren. Die *Deutsche Bahn* erprobt die Technologie für eine effizientere Zugauslastung und erwartet Effizienzsteigerungen bei der Netzauslastung.⁵¹

Das Startup *Zapata* demonstriert mit seinen branchenübergreifenden Projekten in Chemie, Pharma und Logistik das breite Einsatzspektrum dieser revolutionären Technologie – so konnte beispielsweise die Entwicklungszeit für neue Katalysatoren in der chemischen Industrie von durchschnittlich zwei Jahren auf drei Monate verkürzt werden. Diese ersten Erfolge zeigen das immense Potential der Quantentechnologie für praktische Anwendungen.



Die Quantentechnologie wird die nächste industrielle Revolution einläuten.

Jürgen Mlynek, ehemaliger Präsident der *Helmholtz-Gemeinschaft*⁵⁰



Die Transformationskraft des Quantencomputing erstreckt sich über zahlreiche Schlüsselbranchen und verspricht fundamentale Veränderungen in etablierten Prozessen: In der Chemie- und Pharmaindustrie ermöglicht sie die Entwicklung wirksamerer Medikamente durch präzise Molekülsimulationen, wobei die Entwicklungskosten pro Wirkstoff von durchschnittlich 2,5 Mrd. EUR um bis zu 25 % reduziert werden können.



Quantencomputing wird die Art und Weise, wie wir Medikamente entwickeln, revolutionieren.

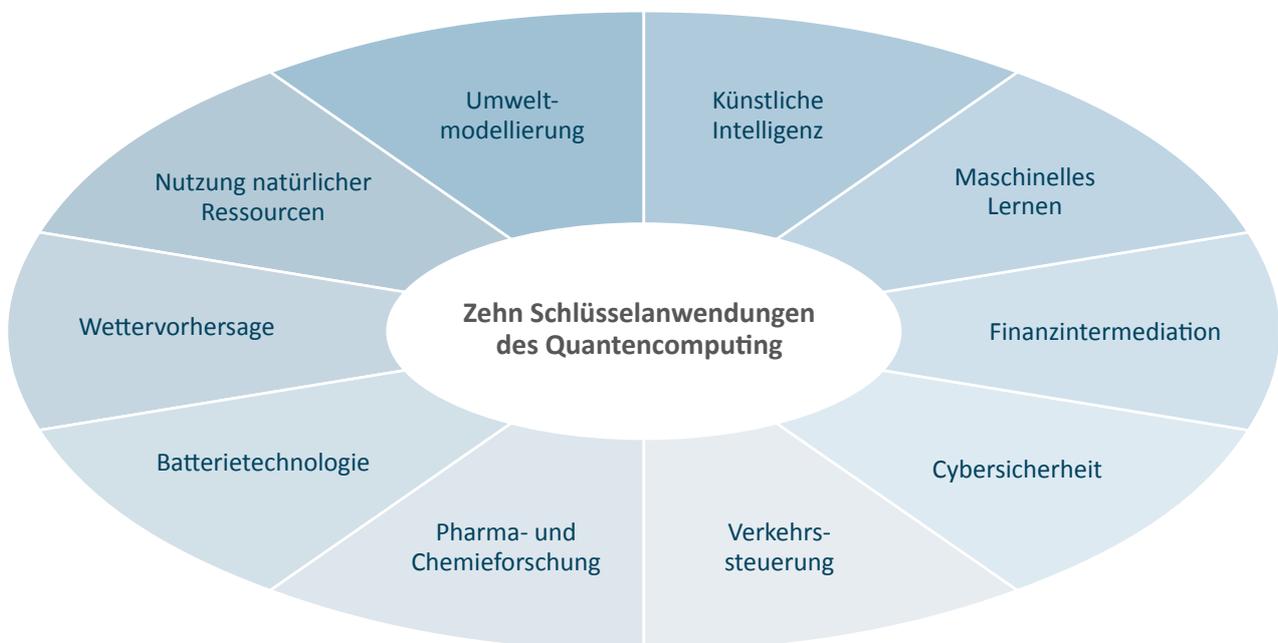
Dario Gil, Direktor bei IBM Research⁵²



Die Automobilindustrie optimiert damit Produktionsabläufe und die Entwicklung autonomer Fahrsysteme – Simulationen, die auf klassischen Computern Monate dauern, können in Stunden durchgeführt werden.⁵³ In der Energiewirtschaft treiben Quantenalgorithmen die Entwicklung effizienterer Batterien und intelligenterer Stromnetze voran, wobei Effizienzsteigerungen von 30 bis 40 % bei der Energiespeicherung erwartet werden.⁵⁴ Logistikunternehmen können komplexe Lieferketten in Echtzeit optimieren und dabei Kosteneinsparungen von bis zu 15 % erzielen.⁵⁵ Diese Anwendungen versprechen nicht nur technologische Fortschritte, sondern auch erhebliche wirtschaftliche Vorteile durch reduzierte Entwicklungszeiten und -kosten, die sich bereits in den nächsten drei bis fünf Jahren manifestieren könnten.

Praktische Anwendungen des Quantencomputing erstrecken sich industrieübergreifend über zehn wichtige Schlüsselanwendungen (Abb. 8).⁵⁶ Im Bereich der Künstlichen Intelligenz ermöglicht die parallele Datenverarbeitung eine bedeutende Beschleunigung von Optimierungsprozessen, während beim maschinellen Lernen die Verarbeitungsgeschwindigkeit

Abb. 8: Industrieübergreifende Schlüsselanwendungen des Quantencomputing



Quelle: Veritis (2024, Quantencomputing-Anwendungen)

komplexer Algorithmen exponentiell gesteigert wird. Für die Finanzbranche eröffnen sich durch präzisere Anlageanalysen und Risikobewertungen neue Möglichkeiten der Portfoliooptimierung. Die Cybersicherheit profitiert von neuartigen Verschlüsselungsmethoden zum Schutz sensibler Daten. Im Verkehrswesen ermöglicht die Echtzeitverarbeitung von Daten eine simultane Optimierung ganzer Fahrzeugflotten.



Auf lange Sicht werden Quantencomputer zusammen mit Quantum Sensing nicht nur eine individualisierte Medizin liefern können, sondern auch ein individualisiertes Wirkstoffdesign basierend auf der individuellen DNA ermöglichen.

Pfeiffer et al. (2021, Quantum Computing)



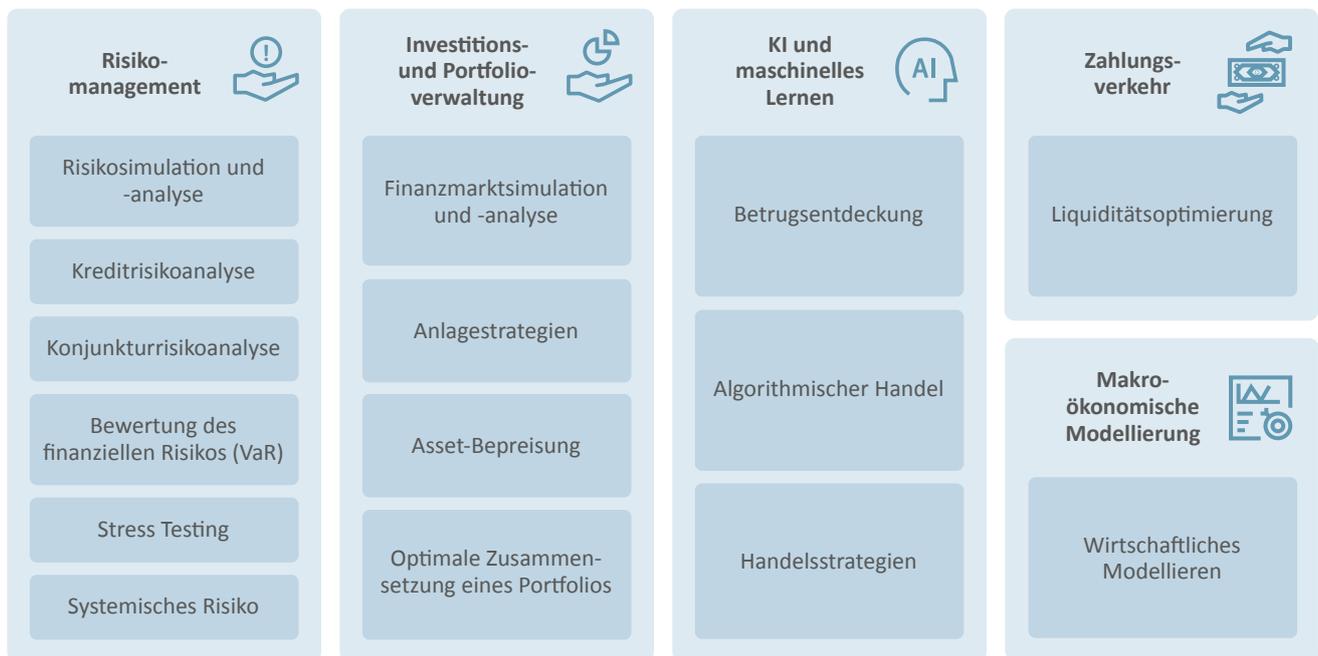
Die Pharma- und Chemieforschung erfährt durch verbesserte Modellierung atomarer Wechselwirkungen einen bedeutenden Entwicklungsschub. In der Batterietechnik führt die fortgeschrittene Materialforschung zu optimierter Leistungsfähigkeit von Energiespeichern und Halbleitern. Die Wettervorhersage gewinnt durch schnellere Datenverarbeitung und präzisere Klimamodelle an Genauigkeit. Die Ressourcennutzung verschiedener Wirtschaftszweige wird durch verbesserte Prozessoptimierung effizienter gestaltet. Nicht zuletzt ermöglicht die präzisere Modellierung von Umweltsystemen genauere Prognosen für Klimawandel und Biodiversität, was zielgenauere Maßnahmen in Bereichen wie Umwelt- und Klimaschutz ermöglicht. Insgesamt wird deutlich, dass Quantencomputing zu einem Schlüsselfaktor für die digitale Transformation der Wirtschaft wird.

Auch für das Zukunftsfeld *New Space*, also die verstärkte kommerzielle Nutzung des Weltraums, ergeben sich aus einem Einsatz von Quantencomputern signifikante Verbesserungsmöglichkeiten:

Nach Ansicht von *Dr. Robert Axmann*, Leiter der Quantencomputing-Initiative des *Deutschen Zentrums für Luft- und Raumfahrt (DLR)*, eignet sich Quantencomputing besonders zur Lösung klassischer Optimierungsprobleme, wie sie zum Beispiel in der Luft- und Raumfahrt auftreten.⁵⁷

Abb. 9 veranschaulicht das breite Spektrum der Anwendungen des Quantencomputing in der Finanzwirtschaft in fünf Kernbereichen: Im Risikomanagement ermöglicht die Technologie die simultane Bewertung tausender Marktszenarien und die Durchführung von Stresstests mit bisher unerreichter Komplexität. Dabei können Wechselwirkungen zwischen Zinsänderungen, Währungsschwankungen und Marktvolatilitäten in Echtzeit analysiert werden. Im Portfoliomanagement optimieren Quantenalgorithmen die Vermögensallokation über multiple Anlageklassen hinweg und berücksichtigen dabei simultan Faktoren wie Liquidität, Transaktionskosten und Steuern. Der Hochfrequenzhandel profitiert von der Fähigkeit, Arbitragemöglichkeiten über globale Märkte hinweg in Mikrosekunden zu identifizieren. In der Betrugs-erkennung kombinieren Quantensysteme Transaktionsmuster mit biometrischen Daten und Verhaltensprofilen für eine präzisere Früherkennung. Für die makroökonomische Modellierung erschließt die Technologie neue Dimensionen, indem sie komplexe Wechselwirkungen zwischen Geldpolitik, Inflation und Wirtschaftswachstum unter Einbeziehung von Millionen von Datenpunkten simuliert.

Abb. 9: Potentielle Vorteile des Quantencomputing im Finanzsektor



Quelle: Auer et al. (2024, Quantum im Finanzwesen)

5.2 Praktische Überlegungen für die Implementierung von Quantentechnologie

Um das Potential der Quantentechnologien zu heben, müssen Unternehmen frühzeitig Strategien entwickeln und umsetzen.⁵⁸ Dabei ist eine enge Verzahnung von Business und Technologie entscheidend. Zunächst sollten relevante Anwendungsfälle identifiziert, priorisiert und auf ihre Eignung für Quantencomputing geprüft werden. Quanten- und Fachexperten müssen eng zusammenarbeiten, um Prototypen zu entwickeln und zu testen. Außerdem müssen interne Kompetenzen auf- und ausgebaut werden. Dies kann durch Trainings, Zukäufe und Kooperationen mit Technologieanbietern und Startups geschehen. Schließlich muss die nötige IT-Infrastruktur für hybride Systeme geschaffen und Quantencomputing schrittweise in die Geschäftsprozesse integriert werden. Dabei sind auch rechtliche und regulatorische Aspekte frühzeitig zu adressieren.

5.3 Mögliche Quantum-Auswirkungen auf die Kryptographie

Quantencomputing und andere aufkommende Anwendungen der Quantenphysik stellen gleichzeitig sowohl Herausforderungen als auch Chancen für die Kryptographie dar – und damit für die Sicherheit und Stabilität von Finanzsystemen sowie generell allen Bereichen mit hoher Datenschutzsensitivität.

“
Die Zukunft der Kryptographie
liegt in der Quantenwelt.

Peter Shor, Mathematiker am MIT⁵⁹

”

Es folgen ein Überblick über die in heutigen Systemen verwendeten kryptographischen Methoden sowie eine Beschreibung der wichtigsten Chancen und Herausforderungen, die eine Anwendung der Quantenphysik hierbei impliziert.

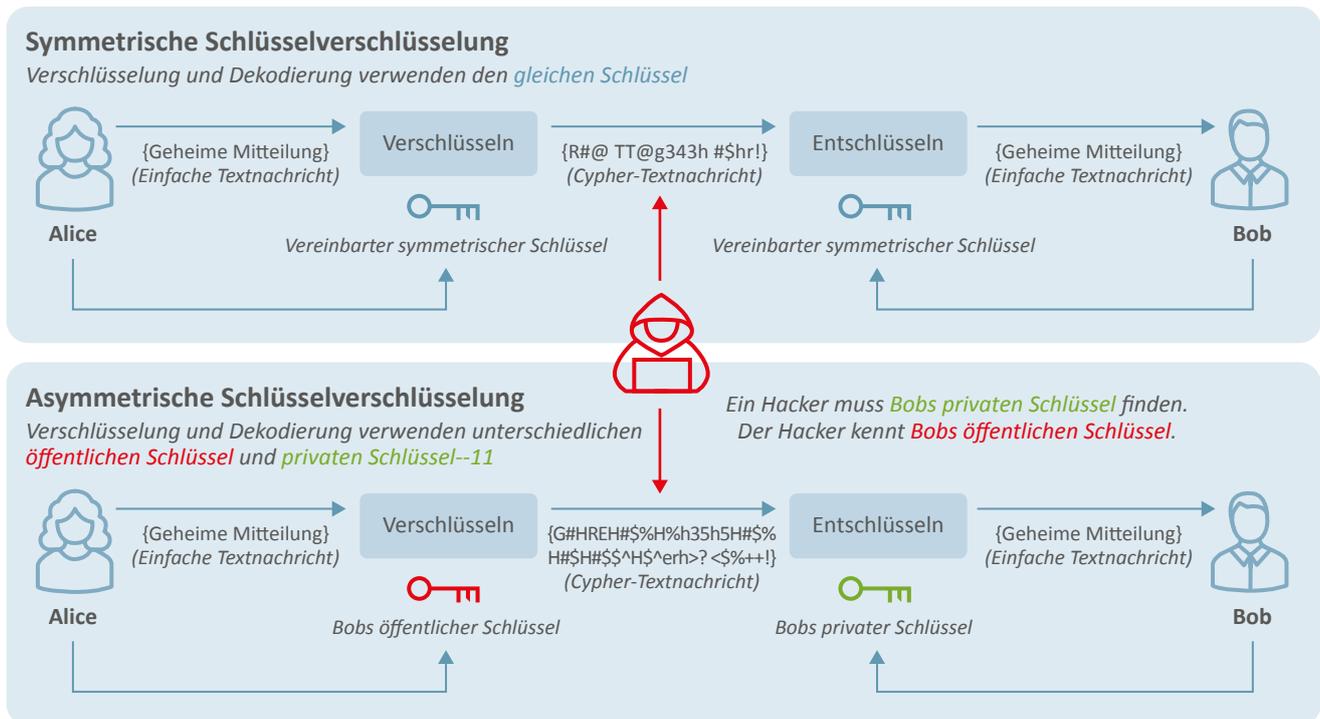
5.3.1 Kryptographie in heutigen Finanzsystemen

Die konventionelle Kryptographie verwendet Algorithmen, die auf komplexen mathematischen Problemen basieren, um sensible Daten zu schützen. Zwei kommunizierende Einheiten verlassen sich in der Regel auf einen gemeinsamen geheimen Schlüssel, um ihre Nachrichten vor Abhören zu schützen. Dies wird als *symmetrische Verschlüsselung* bezeichnet. Der Sender verwendet den gemeinsamen Schlüssel zur Verschlüsselung der Information, und der Empfänger verwendet denselben Schlüssel zur Entschlüsselung der empfangenen Information und zur Wiederherstellung der ursprünglichen Nachricht. Die für die Ver- und Entschlüsselung verwendeten Algorithmen sind standardisiert, und nur der Schlüssel wird geheim gehalten.

Eine Herausforderung bei der **symmetrischen Kryptographie** ist die Notwendigkeit, das gemeinsame Geheimnis zwischen den kommunizierenden Einheiten zu erstellen. Traditionell hätten sie sich im Voraus auf einen gemeinsamen Schlüssel einigen müssen, indem sie den Schlüssel physisch von einem Endpunkt zum anderen übertragen, zum Beispiel auf Papier oder auf einem elektronischen Gerät. In heutigen digitalen Systemen wird dieser anfängliche Schritt in der Regel durch die Erstellung eines gemeinsamen Geheimnisses mittels *Public-Key-Kryptographie*, auch bekannt als **asymmetrische Kryptographie**, ersetzt.

Abb. 10 veranschaulicht den Unterschied zwischen *symmetrischer* und *asymmetrischer Kryptographie*. In einem symmetrischen Szenario, das im oberen Teil der Abbildung dargestellt ist, einigen sich die Nutzer Alice und Bob darauf, einen gemeinsamen Schlüssel für die Ver- und Entschlüsselung ihrer geheimen Nachrichten zu verwenden. Alice verschlüsselt die geheimen Nachrichten mit dem gemeinsamen Schlüssel und sendet sie an Bob. Beim Empfang der verschlüsselten Nachrichten entschlüsselt Bob sie mit demselben gemeinsamen Schlüssel.

Abb. 10: Unterschied zwischen symmetrischer und asymmetrischer Schlüsselverschlüsselung



Quelle: Petrlc et al. (2022, Datenschutz)

Bei der asymmetrischen Kryptographie, dargestellt im unteren Teil von Abb. 10, besitzen Alice und Bob jeweils zwei verschiedene Schlüssel: einen öffentlichen Schlüssel und einen entsprechenden privaten Schlüssel. Wie der Name schon sagt, ist ein öffentlicher Schlüssel für jeden zugänglich, während ein privater Schlüssel vertraulich bleibt. Es ist nicht möglich, einen privaten Schlüssel durch Analyse seines öffentlichen Gegenstücks abzuleiten. Alice verschlüsselt geheime Nachrichten mit Bobs öffentlichem Schlüssel. Wenn Bob verschlüsselte Nachrichten von Alice erhält, entschlüsselt er sie mit seinem privaten Schlüssel.

Die *Public-Key-Kryptographie* erfordert kein gemeinsames Geheimnis zwischen den kommunizierenden Endpunkten; daher entfällt die Notwendigkeit, den Schlüssel vor der geheimen Kommunikation zu übertragen. Stattdessen können die kommunizierenden Einheiten einfach ihre öffentlichen Schlüssel veröffentlichen, die von jedem verwendet werden können, der ihnen verschlüsselte Nachrichten senden möchte.

Bei der *Public-Key-Kryptographie* besteht die Herausforderung darin: Wie kann Alice sicher sein, dass der öffentliche Schlüssel, den sie verwendet, tatsächlich Bob gehört? Was, wenn ein Hacker, der sich als Bob ausgibt, Alice seinen eigenen öffentlichen Schlüssel sendet, um die geheimen Nachrichten abzufangen? Um die Authentizität des öffentlichen Schlüssels zu überprüfen, wird eine *Public-Key-Infrastruktur (PKI)* verwendet, die digitale Zertifikate und *Public-Key-Verschlüsselung* verwaltet. Digitale Zertifikate sind elektronische Dokumente, die von einer Zertifizierungsstelle ausgestellt werden, um die Übereinstimmung zwischen der Identität einer Entität und ihrem öffentlichen Schlüssel zu beweisen.

Wenn Alice überprüfen möchte, ob Bobs öffentlicher Schlüssel tatsächlich Bob gehört, muss sie ein digitales Zertifikat erhalten, das Bobs öffentlichen Schlüssel als legitim authentifiziert. Damit Bob sein digitales Zertifikat erhält, muss er seine Identität und seinen öffentlichen Schlüssel bei einer Zertifizierungsstelle einreichen, einer vertrauenswürdigen Drittorganisation, die Bobs Zertifikat ausstellt. Dieses digitale Zertifikat enthält eine digitale Signatur, die Bobs Eigentum an seinem öffentlichen Schlüssel bestätigt. Die digitale Signatur wird durch Verschlüsselung der Nachricht mit dem privaten Schlüssel der Zertifizierungsstelle erstellt. Alice und andere können bestätigen, dass die digitale Signatur authentisch ist, indem sie die Signatur mit dem öffentlichen Schlüssel der Zertifizierungsstelle entschlüsseln, der auf ihren IT-Geräten gespeichert ist.

In heutigen Finanzsystemen und tatsächlich in den meisten IT-Systemen beruht die Sicherheit auf einer Kombination aus symmetrischer Verschlüsselung, *Public-Key-Kryptographie* und *PKI*. Die meisten Nachrichten werden durch symmetrische Verschlüsselung verschlüsselt, da diese effizienter ist als asymmetrische Verschlüsselung. Allerdings wird asymmetrische Verschlüsselung verwendet, um das gemeinsame Geheimnis zwischen den kommunizierenden Entitäten zu erstellen, bevor eine Kommunikationssitzung beginnt. Und *PKI* wird verwendet, um die Authentizität von öffentlichen Schlüsseln zu überprüfen.

5.3.2 Quantenbedrohung für herkömmliche Kryptographie

Sowohl symmetrische als auch asymmetrische Verschlüsselung basieren auf mathematischen Algorithmen, um Nachrichten mit den jeweiligen Schlüsseln zu ver- und entschlüsseln. Die Algorithmen sind so konstruiert, dass es durch Untersuchung der verschlüsselten Version der Nachricht „praktisch“ unmöglich ist, die ursprüngliche Nachricht oder den geheimen Schlüssel abzuleiten. Theoretisch gibt es Algorithmen, die die Kryptographie brechen und den geheimen Schlüssel herausfinden können, aber bei ausreichend großen Schlüsseln würde dies selbst für die größten Supercomputer eine unvermeidbar lange Rechenzeit erfordern. Daher gilt die konventionelle Kryptographie allgemein als ausreichend sicher für die heutigen Bedürfnisse.

Das Aufkommen von Quantencomputern bringt in dieser Hinsicht eine Veränderung, da sie einige dieser Berechnungen schneller als klassische Computer durchführen können und damit möglicherweise die aktuelle Sicherheit obsolet machen. Das Problem betrifft die asymmetrische Verschlüsselung stärker als symmetrische Verfahren.

Aus diesem Grund konzentriert sich ein erheblicher Teil der Forschungsanstrengungen im Bereich Quantencomputing auf die Frage, wie bestehende Verschlüsselungsverfahren gegen mögliche Angriffe mit QCs abgesichert werden

können (*Quantum-Safe Cryptography*); gleichzeitig steht aber auch die Frage im Raum, durch welche Ansätze in Zukunft „quantensichere“ Verschlüsselungsverfahren erzeugt und implementiert werden können (*Post-Quantum Cryptography*).⁶⁰

Erfahren Sie mehr über die **Postquantenkryptographie** in diesem Video der *Universität St. Gallen*.



Für symmetrische Verschlüsselung kann ein Quantenalgorithmus namens *Grover-Algorithmus* für Angriffe verwendet werden.⁶¹ Dieser Algorithmus kann jedoch im Vergleich zu Angriffen mit einem traditionellen Computer nur eine begrenzte Beschleunigung erreichen. Daher glauben Sicherheitsexperten, dass bestehende symmetrische Verschlüsselung weiterhin verwendet werden kann – vorausgesetzt, die Schlüssellänge wird erhöht.⁶²

QCs haben einen tiefgreifenderen Einfluss auf die asymmetrische Verschlüsselung, bei der einige bestehende Algorithmen nicht mehr sicher sein werden, wenn skalierbare QCs existieren. Insbesondere *Public-Key-Kryptographiemethoden* wie *Rivest-Shamir-Adleman (RSA)* und *Elliptic Curve Cryptography (ECC)*, die in heutigen Finanzsystemen weit verbreitet sind, laufen Gefahr, mit dem Aufkommen von QCs obsolet zu werden.

Ein **skalierbarer Quantencomputer** bezeichnet ein System, das die kontrollierte Erweiterung der Qubit-Anzahl bei gleichbleibender Rechengenauigkeit ermöglicht und damit die Bearbeitung praxisrelevanter Problemstellungen erlaubt. Die zentrale Herausforderung liegt in der Aufrechterhaltung der Quantenkohärenz bei steigender Qubit-Zahl, was derzeit durch Fortschritte in der Fehlerkorrektur und verbesserte Fertigungsprozesse adressiert wird. Experten gehen davon aus, dass für wirtschaftlich relevante Anwendungen mindestens 1.000 fehlerkorrigierte Qubits erforderlich sind – zum Vergleich: Die aktuell leistungsfähigsten Systeme von *IBM* verfügen über 433 physische Qubits. Die Skalierbarkeit gilt als entscheidender Faktor für den kommerziellen Durchbruch der Quantencomputer und bestimmt maßgeblich die Investitionsentscheidungen der Technologiekonzerne.

RSA-Verschlüsselung basiert auf einem mathematischen Problem namens Faktorisierung. Um die Schlüssel zu erstellen, generiert der Algorithmus zufällig zwei große Primzahlen und multipliziert sie dann miteinander. Das Produkt dieser Multiplikation bildet einen Teil des öffentlichen Schlüssels, während die beiden großen Primzahlen zur Generierung des privaten Schlüssels verwendet werden. Die Sicherheit dieses Algorithmus kommt von der Einwegnatur dieser Operation: Die Multiplikation zweier großer Zahlen ist einfach, aber die Faktorisierung großer Zahlen ist mit klassischen Computern sehr schwierig und wird bei ausreichend großen Zahlen praktisch unmöglich. Die Faktorisierung ist jedoch einer der Bereiche, in denen QCs potentiell deutlich leistungsfähiger sein werden als heutige Computer.⁶³



Verschlüsselungen zu durchbrechen ist eine der Anwendungen von Quantencomputern, die die höchste Entwicklungsgeschwindigkeit aufweisen.

Pfeiffer et al. (2021, Quantum Computing)



Der Mathematiker *Peter Shor* zeigte, dass ein ausreichend großer QC die Faktorisierung in angemessener Zeit durchführen und verwendet werden könnte, um derzeit weit verbreitete Verschlüsselungsalgorithmen zu brechen.⁶⁴ Im Jahr 2001 demonstrierten Forscher die praktische Durchführbarkeit von *Shors* Algorithmus, was das Potential von QCs, einige bestehende Cybersicherheitsmaßnahmen unsicher zu machen, weiter unterstrich.

Die Fähigkeit von QCs, heutige kryptographische Systeme zu hacken, hat tiefgreifende Auswirkungen auf die Sicherheit von Finanzsystemen sowie – ganz generell – auch von Kommunikations- und Datenübertragungssystemen. *Deodoro et al.* (2021)⁶⁵ identifizieren die anfälligsten Bereiche als:

- (1) Online-/Mobile-Banking,
- (2) Zahlungstransaktionen (einschließlich Bargeldabhebungen),
- (3) Business-to-Business-Privatsphäre und
- (4) Virtual Private Network (VPN) Kommunikation.

Beim Online-/Mobile-Banking könnte ein Angreifer mit einem QC die Kommunikation zwischen Benutzern und Finanzinstituten während der Authentifizierungs- und Autorisierungsprozesse kompromittieren und abhören. Ähnlich könnten bei Zahlungstransaktionen oder Geldautomatenabhebungen solche Angreifer diese Austausche abfangen. Unternehmen verwenden oft sichere Kommunikationskanäle, die auf Public-Key-Verschlüsselung basieren; diese Kanäle könnten jedoch von Angreifern vollständig zugänglich gemacht werden, wenn sie mit Quantencomputertechniken kompromittiert werden. VPNs, die von Remote-Mitarbeitern verwendet werden, könnten ebenfalls für diese Angriffe anfällig sein.

Es versteht sich von selbst, dass die potentielle Fähigkeit von Quantencomputern, selbst komplexe Verschlüsselungsverfahren zu überwinden, auch für strategisch relevante Bereiche wie **Politik**, **Militär** und **globale Datenkommunikation** von höchster Brisanz ist. Sollte es geopolitisch motivierten Akteuren (wie etwa China oder Nordkorea) gelingen, leistungsfähige Quantencomputer erfolgreich zur Entschlüsselung militärischer oder politischer Kommunikationswege von potentiellen Gegnern einzusetzen, wären je nach Szenario massive Datenlecks und Sicherheitslücken die Folge – mit unabsehbaren Konsequenzen für die jeweilige Verteidigungsfähigkeit im Konfliktfall.⁶⁶

- Dieser Aspekt gilt in besonderem Maße für den immer intensiver ausgetragenen globalen Machtkampf im Weltraum („*Space Cold War*“), der selbst für militärisch führende Großmächte wie die USA völlig neue Bedrohungsszenarien mit sich bringt.⁶⁷

Die Risiken latent zunehmender Konflikte im Weltraum analysiert das FERI Institut in dem Cognitive Comment „*Space Cold War: Massive Militarisierung des Weltraums als globales Risiko*“.

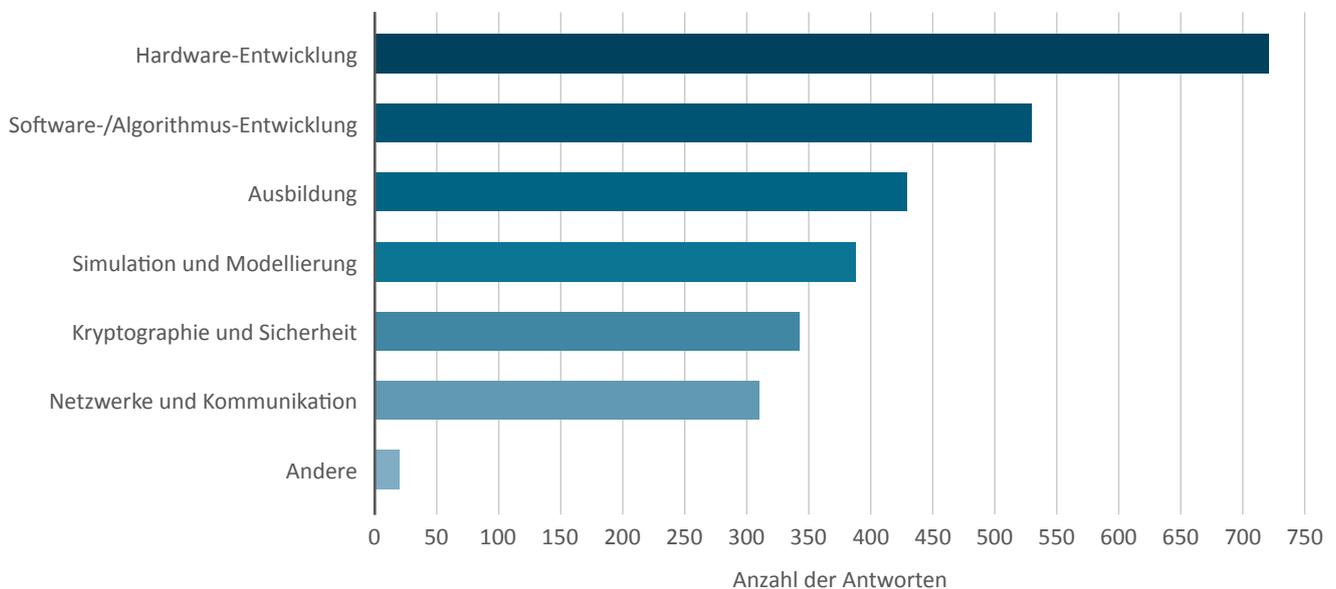


6 Quantentechnologie für Investoren

6.1 Investitionsmöglichkeiten in der Quantentechnologie-Branche

Für Investoren eröffnet Quantencomputing attraktive Möglichkeiten (Abb. 11).⁶⁸ So können sie direkt in Hardware-Hersteller wie *IonQ*, *D-Wave* oder *Rigetti* investieren, die Quantenprozessoren entwickeln. Aussichtsreich sind auch Unternehmen, die Quantenalgorithmen entwickeln und in Softwarelösungen umsetzen, wie *1Qbit*, *Zapata*, *Cambridge Quantum Computing* und *QC Ware*. Wachstumschancen bieten zudem Anbieter quantenresistenter Kryptographie wie *Post-Quantum* und Anbieter von Komponenten wie Kühlsystemen. Auch Unternehmenspartnerschaften und Risikokapitalfonds, die in Quanten-Startups investieren, sind interessant.

Abb. 11: Benötigte Investitionsschwerpunkte zur Förderung des Quantencomputing



Quelle: QuEra Computing (2024, Umfrage)

6.2 Markttrends und Wachstumspotential

Die globale Expansion von Computing-Diensten wurde durch den COVID-19-Ausbruch erheblich beeinflusst. Der Anteil privater und risikokapitalfinanzierter Investitionen in Quantencomputing stieg in der zweiten Hälfte des Jahres 2021 deutlich an.⁶⁹ Dieser Anstieg machte über 70 % der Investitionen aus, was auf einen wachsenden Glauben der Unternehmen an die potentiellen Vorteile der Technologie hindeutet.⁷⁰ Daher wird erwartet, dass unter Berücksichtigung der oben genannten Faktoren speziell Künstliche Intelligenz, Cloud Computing und andere innovative Ansätze die disruptiven Technologien sein werden, die zukünftige Plattformen ermöglichen.

Die globale Marktgröße für Quantencomputing wurde im Jahr 2023 auf 885,4 Mio. USD geschätzt und wird voraussichtlich von 1.160,1 Mio. USD im Jahr 2024 auf 12.620,7 Mio. USD bis 2032 wachsen, was einer CAGR von 34,8 % während des Prognosezeitraums entspricht.⁷¹ Die Region Nordamerika dominierte den globalen Markt mit einem Anteil von 43,86 % im Jahr 2023.⁷²

6.3 Risiken und Herausforderungen für Investoren in der Quantentechnologie

Quantencomputing ist derzeit noch eine unreife Technologie mit vielen Unwägbarkeiten.⁷³ Noch ist unklar, welche der konkurrierenden Plattformen sich durchsetzen wird. Auch die Entwicklung skalierbarer und robuster Fehlerschutzmechanismen sowie praktikabler Software steht noch am Anfang. Neben technologischen bestehen auch kommerzielle Risiken. Da viele Anwendungsszenarien noch nicht erprobt sind, könnten sich Geschäftsmodelle als nicht tragfähig erweisen.

Investitionen in Startups stehen vor einer kritischen Phase zwischen der Forschungsarbeit und der erfolgreichen Markteinführung ihrer Produkte und Dienstleistungen. Wettbewerbsvorteile durch Quantencomputing könnten sich als nicht nachhaltig erweisen, wenn Konkurrenten aufholen. Auch regulatorische Einschränkungen, etwa beim Zugriff auf Quantencomputer, sind ein Risiko.

Investoren sollten sich der folgenden Risiken und Herausforderungen bewusst sein:

Tab. 2: Risiken und Herausforderungen für Investoren

Risikokategorie	Beschreibung
Technologische Unsicherheit	<ul style="list-style-type: none"> • Unklarheit über die dominierende Plattform • Herausforderungen bei der Entwicklung skalierbarer Fehlerschutzmechanismen • Mangel an ausgereifter Quantensoftware
Kommerzielle Risiken	<ul style="list-style-type: none"> • Unerprobte Anwendungsszenarien • Mögliche Nicht-Tragfähigkeit von Geschäftsmodellen • Kritische Phase zwischen Forschung und Kommerzialisierung
Wettbewerbsrisiken	<ul style="list-style-type: none"> • Potenziell kurzlebige Wettbewerbsvorteile • Schnelles Aufholen der Konkurrenz
Regulatorische Risiken	<ul style="list-style-type: none"> • Mögliche Einschränkungen beim Zugriff auf Quantencomputer • Unvorhersehbare gesetzliche Rahmenbedingungen
Finanzielle Risiken	<ul style="list-style-type: none"> • Hohe Anfangsinvestitionen • Lange Amortisationszeiten • Unsichere Renditeaussichten

Quelle: Blaschke (2024, Quantencomputing)

Angesichts dieser Risiken ist es für Investoren ratsam, einen langfristigen Anlagehorizont zu wählen und Kapital diversifiziert zu investieren. Eine gründliche Due-Diligence-Prüfung und kontinuierliche Marktbeobachtung sind dabei unerlässlich. Trotz großer Herausforderungen bietet die Quantentechnologie enorme Chancen – auch für risikobereite und zukunftsorientierte Investoren.

6.4 Die geopolitische Dimension des Quantencomputing

Quantencomputer versprechen, viele komplexe Berechnungen exponentiell schneller durchführen zu können als herkömmliche Computer. Dies hat potentiell revolutionäre Auswirkungen auf zahlreiche Bereiche wie Kryptographie, Medikamentenentwicklung, Materialwissenschaften, Finanzmodellierung und Künstliche Intelligenz. Angesichts dieser weitreichenden Implikationen investieren führende Nationen massiv in die Quantentechnologie, um sich einen strategischen Vorteil in der globalen Technologie- und Wirtschaftslandschaft zu verschaffen (vgl. Abb. 12).⁷⁴

6.4.1 Investitionen in Forschung und Entwicklung

Die Vereinigten Staaten sind derzeit führend bei Investitionen in Quantencomputing (vgl. Abb. 12). Der *National Quantum Initiative Act*, der 2018 verabschiedet wurde, stellte initial über 1,2 Mrd. USD für die Quantenforschung bereit. Seitdem wurden die Investitionen weiter erhöht. Im August 2022 unterzeichnete Präsident *Biden* zwei Direktiven zur Förderung der Quantentechnologie, die zusätzliche Mittel und eine verstärkte Koordination der Forschungsanstrengungen vorsehen.⁷⁵ Die Vereinigten Staaten behaupten dadurch ihre führende Position in der Quantentechnologie durch weitere massive öffentliche und private Investitionen von jeweils etwa 3,8 Mrd. USD. Mit 14 großen Forschungszentren im Rahmen der *National Quantum Initiative* und bedeutenden technischen Durchbrüchen, wie *IBMs* 1.121-Qubit-Chip *Condor* und *QuEra Computings* Quantenfehlerkorrektur mit 48 logischen Qubits, demonstriert das Land seine technologische Überlegenheit. Der US-Kongress bekräftigte diese Führungsrolle durch die Verabschiedung des *National Quantum Initiative Reauthorization Act* im November 2023.

China gilt als zweitgrößter Investor und hat ehrgeizige Pläne für die Entwicklung von Quantentechnologien (vgl. Abb. 12). Obwohl genaue Zahlen schwer zu ermitteln sind, schätzen Experten, dass China bis 2030 über 15 Mrd. USD in diesem Bereich investieren wird. Das Land hat Quantentechnologie zu einer der Schlüsseltechnologien in seinem aktuellen Fünfjahresplan erklärt.⁷⁶ Laut dem aktuellen *Quantum-Monitor* von *McKinsey* zeichnet sich folgendes Bild der chinesischen Quantentechnologie-Entwicklung ab:⁷⁷ Die Quantentechnologie-Entwicklung in China wird durch massive staatliche Investitionen von mindestens 15,3 Mrd. USD vorangetrieben, wobei einige Quellen sogar von bis zu 25 Mrd. USD sprechen. Mit 29 spezialisierten Forschungseinrichtungen und bedeutenden Erfolgen wie dem *Origin Wukong Quantencomputer* mit 72 Rechen-Qubits und der Demonstration von Quantenkommunikation über 2.300 Meilen via Satellit zeigt China seine Entschlossenheit, in diesem strategischen Technologiebereich aufzuholen und möglicherweise die globale Führung zu übernehmen.

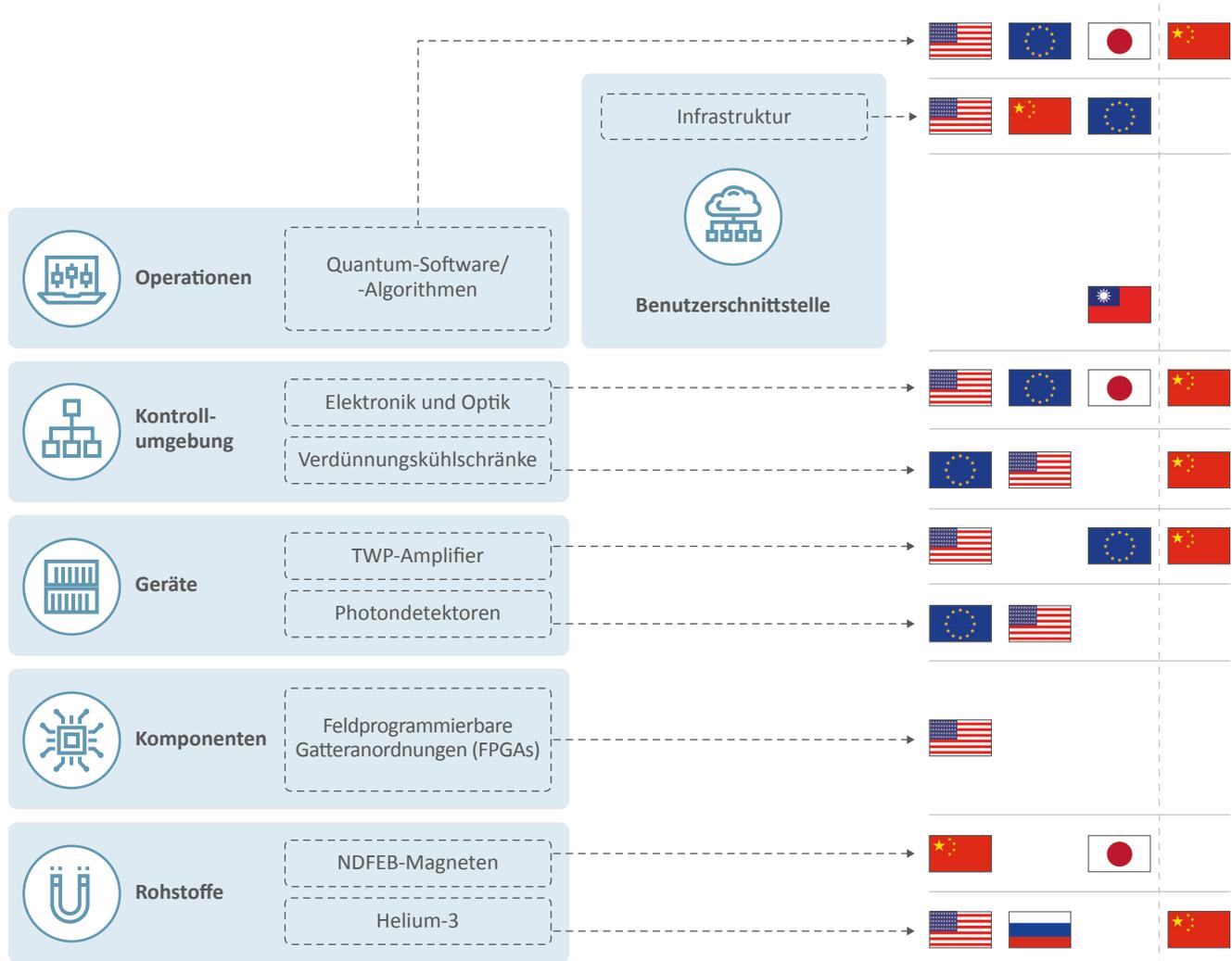
Die Europäische Union hat ein *Quantum Flagship Programm* mit einem Budget von 1 Mrd. EUR über zehn Jahre aufgelegt. Dieses Programm zielt darauf ab, Europa an die Spitze der zweiten Quantenrevolution zu bringen. Zusätzlich investieren einzelne europäische Länder wie Deutschland, Frankreich und die Niederlande erhebliche Summen in ihre nationalen Quantenprogramme.⁷⁸ Außerdem gehören Quantentechnologien in der Verordnung über die Plattformen für *Strategische Technologie für Europa (STEP)* zu den vorrangig behandelten Technologien.

EU-Kommission identifiziert vier kritische Technologiebereiche:

- fortschrittliche Halbleitertechnologien (Mikroelektronik, Photonik, Hochfrequenzchips, Ausrüstung zur Herstellung von Halbleitern);
- Technologien der künstlichen Intelligenz (Hochleistungsrechnen, Cloud- und Edge-Computing, Datenanalyse, maschinelles Sehen, Sprachverarbeitung, Objekterkennung);
- Quantentechnologien (Quanteninformatik, Quantenkryptografie, Quantenkommunikation, Quantenerfassung und -radar);
- Biotechnologien (Verfahren der genetischen Veränderung, neue genomische Verfahren, Gene Drive (Genantrieb), synthetische Biologie).⁷⁹

Der europäische Quantentechnologie-Sektor zeichnet sich durch eine koordinierte, länderübergreifende Strategie aus, wobei Deutschland mit 5,2 Mrd. USD öffentlicher Investitionen und dem Ziel eines universellen Quantencomputers bis 2026 eine Vorreiterrolle einnimmt. Großbritannien investiert 3,1 Mrd. USD über zehn Jahre mit dem Ziel, bis 2033 eine führende Quantenwirtschaft zu werden, während Frankreich mit seinem 1,3-Milliarden-Dollar-Programm über fünf Jahre und dem Ziel von 16.000 neuen Arbeitsplätzen die Industrialisierung der Quantentechnologie vorantreibt. Diese kombinierten Anstrengungen positionieren Europa als starken Konkurrenten im globalen Quantenwettbewerb (vgl. Abb. 12).

Abb. 12: Führende Länder und Regionen der Quantentechnologie



Quelle: Lazzarotto (2024, Geopolitik)

6.4.2 Anwendungen und Patente

Bei Patenten für Quantentechnologien hat China in den letzten Jahren stark aufgeholt und liegt nun vorne. Laut einer Analyse von McKinsey aus dem Jahr 2022 hält China 43 % der Quantenpatente weltweit, gefolgt von den USA mit 22 % und Japan mit 11 %.⁸⁰ Allerdings sind viele chinesische Patente auf Quantenkommunikation und Quantenkryptographie fokussiert, während US-Patente eher Quantencomputer-Hardware und -algorithmen betreffen. Die unterschiedlichen Schwerpunkte in der Patentlandschaft zwischen China und den USA lassen wichtige strategische Schlussfolgerungen zu:

- ▶ China setzt offenbar stark auf abhörsichere Kommunikation und den Schutz sensibler Daten, was sowohl militärische als auch wirtschaftliche Vorteile verspricht. Dies könnte bedeuten, dass China sich gegen potentielle Cybersicherheitsbedrohungen wappnet und gleichzeitig eine führende Position in der sicheren Datenübertragung anstrebt.
- ▶ Ebenso plausibel ist aber auch das Ziel, durch Einsatz modernster Quantentechnologie bestehende Verschlüsselungsverfahren erklärter Systemrivalen (wie die USA) sowie potentieller militärischer Ziele (wie Taiwan) zu kompromittieren oder im Konfliktfall ganz auszuhebeln.

Wie zielstrebig China modernste Technologie für sein Ziel geopolitischer und ökonomischer Dominanz im 21. Jahrhundert einsetzt, hat das FERI Institut mehrfach analysiert, zuletzt in der Studie „**Neue Weltordnung – Made in China**“.



Die USA hingegen konzentrieren sich auf die Entwicklung von Quantencomputern, die das Potential haben, bestehende Verschlüsselungsmethoden zu brechen und komplexe Berechnungen in verschiedenen Bereichen wie Materialwissenschaften, Pharmaforschung und Künstlicher Intelligenz zu revolutionieren. Dies deutet auf eine Strategie hin, durch maximale Rechenleistung die wirtschaftliche und technologische Vormachtstellung zu sichern.

Diese divergierenden Schwerpunkte könnten zu einer asymmetrischen technologischen Entwicklung führen (vgl. Abb. 12): Während China möglicherweise einen Vorsprung in der abhörsicheren Kommunikation aufbaut, könnten die USA einen Vorteil in der Quantencomputing-Leistung entwickeln. Für europäische Unternehmen und Forschungseinrichtungen bedeutet dies, dass Kooperationen mit beiden Regionen wichtig sind, um von beiden Entwicklungsrichtungen zu profitieren.

Bei praktischen Anwendungen und kommerziellen Fortschritten sind US-Unternehmen wie *IBM*, *Google*, *Microsoft* und *Amazon Web Services* führend. *IBM* stellte 2019 den ersten kommerziellen Quantencomputer vor und bietet seitdem Quantenservices über die Cloud an. Das Unternehmen hat kürzlich eine Roadmap vorgestellt, die die Entwicklung von Quantenprozessoren mit über 4'000 Qubits bis 2025 vorsieht.⁶

6.4.3 Internationale Zusammenarbeit und Wettbewerb

Trotz des intensiven Wettbewerbs gibt es auch Bereiche der internationalen Zusammenarbeit im Quantencomputing. Wissenschaftler aus verschiedenen Ländern kooperieren in Forschungsprojekten und auf Konferenzen. Im akademischen Bereich zeigt sich die Kooperation besonders deutlich:

- Das *Indian Institute of Technology (IIT)* Bombay ging 2023 eine Partnerschaft mit dem *Chicago Quantum Exchange* ein, um gemeinsam Forschungsprojekte durchzuführen und Nachwuchskräfte auszubilden.
- Auch auf Unternehmensebene gibt es starke internationale Verflechtungen: *IBM* ist hier besonders aktiv. Das Unternehmen betreibt nicht nur Quantencomputer in den USA, sondern hat 2023 auch Kanadas ersten *Quantum System One* mit 127 Qubits in Québec installiert und plant ein Quantenrechenzentrum in Deutschland.
- Die deutsch-amerikanische Zusammenarbeit wird durch die Ansiedlung des *IBM-Quantenrechenzentrums* in Ehningen verstärkt, wo ab 2024 mehrere Quantensysteme mit jeweils über 100 Qubits betrieben werden sollen.
- Ein weiteres Beispiel ist die Zusammenarbeit zwischen dem koreanischen *KAIST (Korea Advanced Institute of Science and Technology)* und dem französischen Unternehmen *PASQAL*, die 2024 gemeinsam ein Quanten-Ökosystem in der Stadt Sejong aufbauen.

Diese Beispiele zeigen, dass die Quantentechnologie trotz des weltweiten Wettbewerbs ein Bereich ist, in dem internationale Zusammenarbeit aktiv gelebt wird – sowohl zwischen Forschungseinrichtungen als auch zwischen Unternehmen verschiedener Länder.

Allerdings haben geopolitische Spannungen, insbesondere zwischen den USA und China, zu erheblichen Beschränkungen beim Technologietransfer und bei der Zusammenarbeit geführt. Diese Tendenz wird sich weiter verstärken, da Quantencomputing speziell von den Großmächten USA und China als **absolut zukunfts-kritische Technologie** eingestuft wird. Es lassen sich folgende konkrete Beispiele für Einschränkungen in der internationalen Zusammenarbeit erkennen:

- Während China und Russland gemeinsam an Quantenkommunikation über Satelliten arbeiten (wie im Dezember 2023 mit dem *Mozi-Satelliten* über 2.300 Meilen demonstriert), gibt es kaum noch direkte Kooperationen zwischen chinesischen und US-amerikanischen Forschungseinrichtungen im Quantenbereich.
- Die USA setzen verstärkt auf Partnerschaften mit verbündeten Nationen: Dies zeigt sich beispielsweise in der gezielten Zusammenarbeit mit Südkorea, dokumentiert durch eine gemeinsame Erklärung beider Regierungen im April 2023 zur Kooperation in der Quantentechnologie.
- Die jeweiligen Investitionsmuster verdeutlichen das Prinzip der Abschottung: Während die USA etwa 3,8 Mrd. USD private Investitionen verzeichnen, liegt China bei nur 359 Mio. USD *gemeldeten* privaten Investitionen – was darauf hindeutet, dass westliche Investoren zurückhaltend bei Investitionen in chinesische Quantentechnologie sind.
- Auch die unterschiedlichen Forschungsschwerpunkte – USA fokussiert auf Quantencomputing, China auf Quantenkommunikation – können als Folge der eingeschränkten Zusammenarbeit interpretiert werden, da jede Nation eigene, unabhängige Entwicklungspfade verfolgt.
- Dies zeigt sich auch in der Bildung separater Technologie-Ökosysteme: Die USA entwickeln mit Partnern wie *IBM*, *Google* und Start-ups ein eigenes Ökosystem, während China mit Firmen wie *Origin Quantum* und dem *Hefei National High-Tech Industry Development Zone* ein paralleles Ökosystem aufbaut.

6.4.4 Herausforderungen und Zukunftsaussichten

Trotz der enormen Fortschritte steht das Quantencomputing noch vor erheblichen Herausforderungen. Die Hauptprobleme sind die Aufrechterhaltung der Quantenkohärenz, die Skalierung der Systeme und die Entwicklung praktischer Anwendungen. Experten gehen davon aus, dass es noch Jahre oder sogar Jahrzehnte dauern könnte, bis Quantencomputer ihr volles Potential entfalten.⁸¹

Quantenkohärenz beschreibt die empfindliche Eigenschaft von Qubits, ihre quantenmechanischen Zustände und deren Überlagerungen über eine bestimmte Zeitspanne aufrechtzuerhalten. Diese essenzielle Eigenschaft wird durch Wechselwirkungen mit der Umgebung, wie etwa Temperatureinflüsse oder elektromagnetische Störungen, beeinträchtigt – ein Vorgang, der als Dekohärenz bezeichnet wird. Die aktuell erreichten Kohärenzzeiten liegen bei supraleitenden Quantencomputern im Bereich von Mikrosekunden, bei Ionenfallen im Bereich von Millisekunden. Der Erhalt der Quantenkohärenz stellt eine zentrale technologische Herausforderung dar und bestimmt maßgeblich die Leistungsfähigkeit von Quantencomputern in praktischen Anwendungen.

Dennoch investieren Regierungen und Unternehmen weltweit weiterhin massiv in diese Technologie, da sie das Potential hat, ganze Industrien zu transformieren. Quantensensoren und Quantenkommunikation könnten sogar früher praktische Anwendungen finden als vollwertige Quantencomputer.

Das Rennen um die Vorherrschaft im Quantencomputing ist in vollem Gange, mit den USA und China als Hauptkonkurrenten und Europa als wichtigem Akteur. Während China bei Patenten und Publikationen vorne liegt, verteidigen die USA bei praktischen Anwendungen und kommerzieller Umsetzung ihre Pionierrolle. Europa versucht durch koordinierte Forschungsprogramme aufzuholen und seine Stärken in der Grundlagenforschung zu nutzen (vgl. Abb. 12, S. 30).

Für Investoren bietet das Feld des Quantencomputing vielversprechende Möglichkeiten, erfordert aber eine sorgfältige Analyse der technologischen Entwicklungen und des geopolitischen Kontexts. Die langfristigen Gewinner in diesem Bereich werden diejenigen sein, die sich nicht nur mit der Technologie an sich auseinandersetzen, sondern auch mit den vielfältigen praktischen Anwendungsfällen.

Die **geopolitischen Implikationen** des Quantencomputing gehen weit über den technologischen Wettbewerb hinaus. Sie betreffen auch Fragen der nationalen Sicherheit, der wirtschaftlichen Wettbewerbsfähigkeit und der globalen technologischen Standards. In den kommenden Jahren wird es entscheidend sein, wie Nationen und internationale Organisationen Regelungen für die Entwicklung und den Einsatz von Quantentechnologien gestalten.

7 Fazit und Ausblick auf die Zukunft

7.1 Implikationen der Quantentechnologie für Realwirtschaft und Finanzmärkte



Quantencomputer werden die Art und Weise, wie wir über Berechnungen denken, grundlegend verändern.

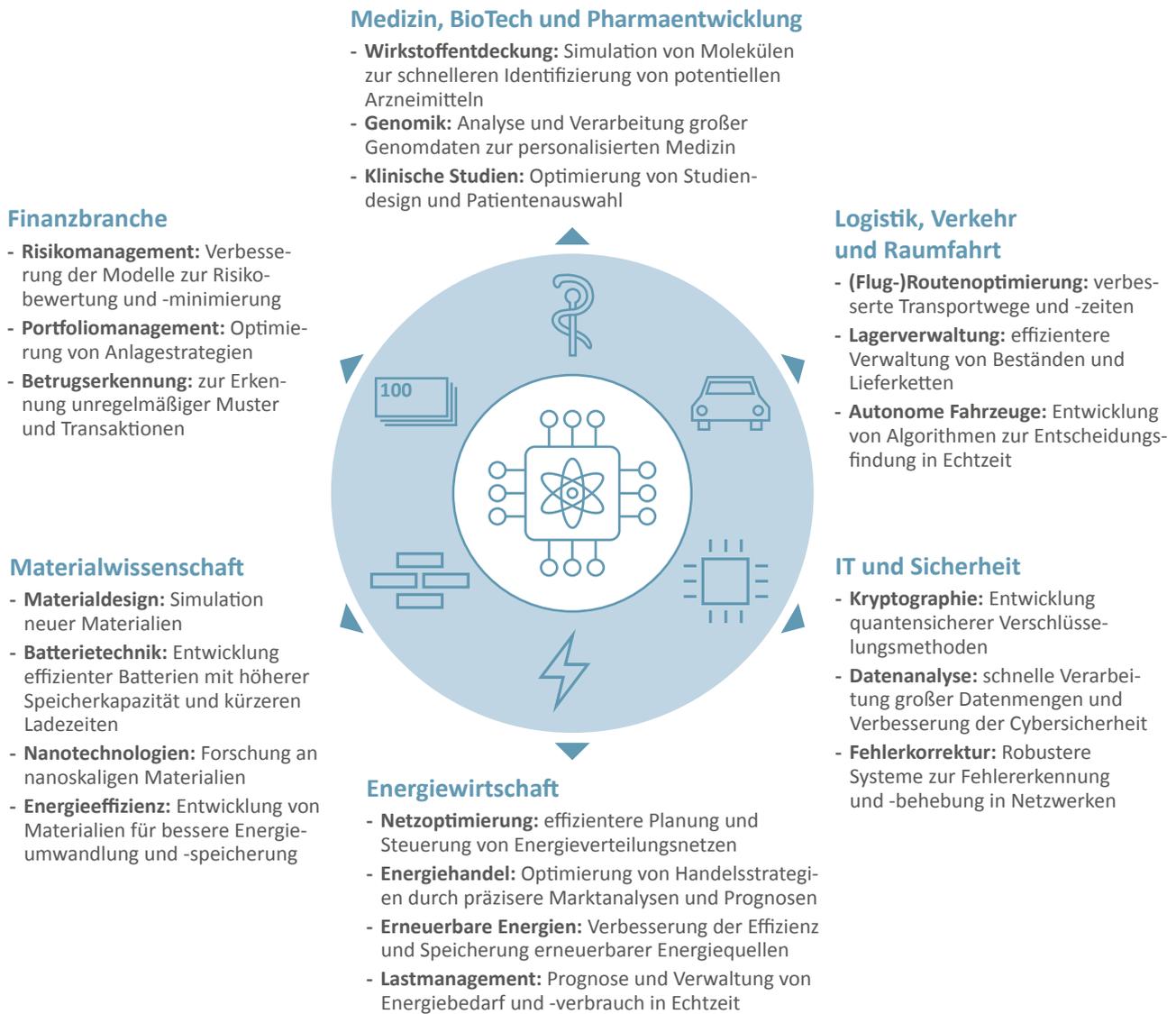
Satya Nadella, CEO von *Microsoft*⁸²



Die Quantentechnologie steht an der Schwelle zu einer weitreichenden kommerziellen Nutzung, die sowohl die Realwirtschaft als auch den Finanzsektor grundlegend transformieren wird. Der aktuelle *McKinsey Quantum Technology Monitor 2024* prognostiziert für das Quantencomputing bis 2035 Marktumsätze von 28 bis 72 Mrd. EUR.⁸³ Diese Entwicklung wird durch erhebliche staatliche Förderungen von insgesamt 42 Mrd. EUR weltweit sowie ein dynamisches Startup-Ökosystem mit aktuell 367 Unternehmen getragen.⁸⁴

Die Implikationen für die Realwirtschaft sind tiefgreifend und branchenübergreifend. Im Chemiesektor zeichnet sich eine Revolution der Materialforschung durch hochpräzise Molekularsimulationen ab. Diese ermöglichen die Entwicklung neuartiger Materialien mit maßgeschneiderten Eigenschaften bei deutlich verkürzten Entwicklungszyklen. Die Automobilbranche profitiert von der Optimierung komplexer Fertigungsprozesse und Lieferketten, wodurch sich Produktionseffizienz und Ressourcennutzung erheblich verbessern lassen. In der Pharmaindustrie beschleunigt die Quantentechnologie die Wirkstoffentwicklung durch verbesserte Proteinfaltungssimulationen, was zu einer signifikanten Verkürzung der Entwicklungszeiten für neue Medikamente führt. Der Maschinenbau erschließt neue Möglichkeiten in der Werkstoffoptimierung und Prozesssteuerung. In der Luft- und Raumfahrt sowie dem gesamten Transport- und Verkehrswesen werden komplexeste Berechnungen in Echtzeit möglich (vgl. Abb. 13, S. 34).

Abb. 13: Die Schlüsseltechnologien des Quantencomputing



► **Neue Lösungen für komplexe Sachverhalte mit vielen Variablen und Abhängigkeiten inkl. einer deutlichen Effizienzsteigerung**

Quelle: FERI Cognitive Finance Institute, 2024; basierend auf Fraunhofer (2024, Quantentechnologien)

Die operativen Auswirkungen auf Unternehmensebene sind weitreichend. Produktentwicklungsprozesse werden grundlegend neu gestaltet, da Quantencomputer komplexe Simulationen und Optimierungen in bisher unerreichbarer Geschwindigkeit durchführen können. In der Logistik entstehen erhebliche Effizienzsteigerungen durch optimierte Routenplanung und Bestandsmanagement. Dies bedeutet auch:

- Unternehmen müssen auf Quantencomputing spezialisierte Abteilungen aufbauen und verstärkt in die Aus- und Weiterbildung ihrer Mitarbeiter investieren, um die neuen technologischen Möglichkeiten optimal nutzen zu können.

Im Finanzsektor zeichnen sich besonders deutliche Veränderungen ab: Das Anlagemanagement erfährt eine fundamentale Transformation durch quantenbasierte Portfoliooptimierung. Die Möglichkeit, komplexe Risikoszenarien in Echtzeit zu simulieren, erlaubt präzisere Risikomodelle und effizientere Anlagestrategien. *Monte-Carlo-Simulationen* werden durch Quantenalgorithmen erheblich verfeinert, wodurch genauere Prognosen und Bewertungen ermöglicht werden. Quantenbasierte Berechnungsmethoden ermöglichen neue Derivatestrukturen, die auch bisher nicht modellierbare Marktszenarien abbilden können.

Doch auch die Finanzmarktinfrastuktur steht vor grundlegenden Anpassungen. Die Umstellung auf **quantensichere Verschlüsselungssysteme** ist unerlässlich, um die Sicherheit von Finanztransaktionen auch in einer Ära leistungsfähiger Quantencomputer zu gewährleisten. Handelsalgorithmen müssen an die neuen Quantencomputing-Kapazitäten angepasst werden, was zu einer Neugestaltung des algorithmischen Handels führt. Die IT-Infrastruktur der Finanzinstitute entwickelt sich in Richtung **hybrider Systeme**, die klassische und quantenmechanische Rechenleistung kombinieren.

Im Finanzsektor könnten neue Geschäftsmodelle durch quantenbasierte Finanzprodukte und spezialisierte Beratungsdienstleistungen entstehen. Es wäre denkbar, dass Banken und Vermögensverwalter maßgeschneiderte Handelsstrategien für Quantencomputing-Akteure entwickeln und entsprechende Expertise aufbauen würden. Die Nachfrage nach Quantenberatung könnte steigen, da Unternehmen möglicherweise Unterstützung bei der Integration der neuen Technologie benötigen würden.

Für den erfolgreichen Übergang zur Quantentechnologie ist eine frühzeitige strategische Positionierung entscheidend. Exponierte Unternehmen – etwa im Bereich der Logistik und Finanzindustrie – müssen schon jetzt gezielt Quantenexpertise aufbauen und in quantenfähige Infrastruktur investieren. Der Aufbau interdisziplinärer Teams und die Entwicklung spezifischer Anwendungsfälle sind zentrale Erfolgsfaktoren. Die größten Chancen liegen in der frühen Adaptation der Technologie und der systematischen Entwicklung branchenspezifischer Lösungen.



Quantencomputer sind nicht dafür gebaut, bestimmte Probleme zu lösen, sie sind eine Plattform und es besteht fast kein Zweifel daran, dass Quantencomputer jeden Markt revolutionieren können.

Pfeiffer et al. (2021, Quantum Computing)



Die Transformation durch Quantentechnologie erfordert auch eine Anpassung der Unternehmenskultur und -organisation. Abteilungsübergreifende Zusammenarbeit und kontinuierliche Weiterbildung werden zu Schlüsselfaktoren für den Erfolg. Betroffene Unternehmen müssen ihre Innovationsprozesse neu ausrichten und flexible Strukturen schaffen, die eine schnelle Integration quantentechnologischer Lösungen ermöglichen.

Der Übergang zur Quantentechnologie wird nicht abrupt, sondern schrittweise erfolgen. In einer ersten Phase werden hybride Lösungen dominieren, die klassische und quantenbasierte Systeme kombinieren. Mit zunehmender technologischer Reife werden reine Quantenlösungen an Bedeutung gewinnen. Unternehmen und Finanzinstitute müssen diese Entwicklung aktiv begleiten und ihre Strategien kontinuierlich anpassen.

Die wirtschaftlichen Potentiale der Quantentechnologie sind erheblich. Neben direkten Effizienzgewinnen und Kosteneinsparungen entstehen völlig neue Geschäftsfelder und Wertschöpfungsmöglichkeiten. Der prognostizierte wirtschaftliche Mehrwert von etwa 2 Bio. EUR bis 2035 verdeutlicht die transformative Kraft dieser Technologie.⁸⁵ Besonders die Schlüsselbranchen Chemie, Biowissenschaften, Finanzen und Mobilität werden von dieser Entwicklung profitieren.

- ▶ Die strategische Bedeutung der Quantentechnologie macht sie zu einem **zentralen Faktor** für die zukünftige Wettbewerbsfähigkeit von Unternehmen und ganzen Volkswirtschaften.
- ▶ Investitionen in Quantentechnologie sind daher nicht nur technologische, sondern auch **strategische Entscheidungen**, die die Positionierung im globalen Wettbewerb maßgeblich beeinflussen werden.

7.2 Prognosen für die Zukunft der Quantentechnologie

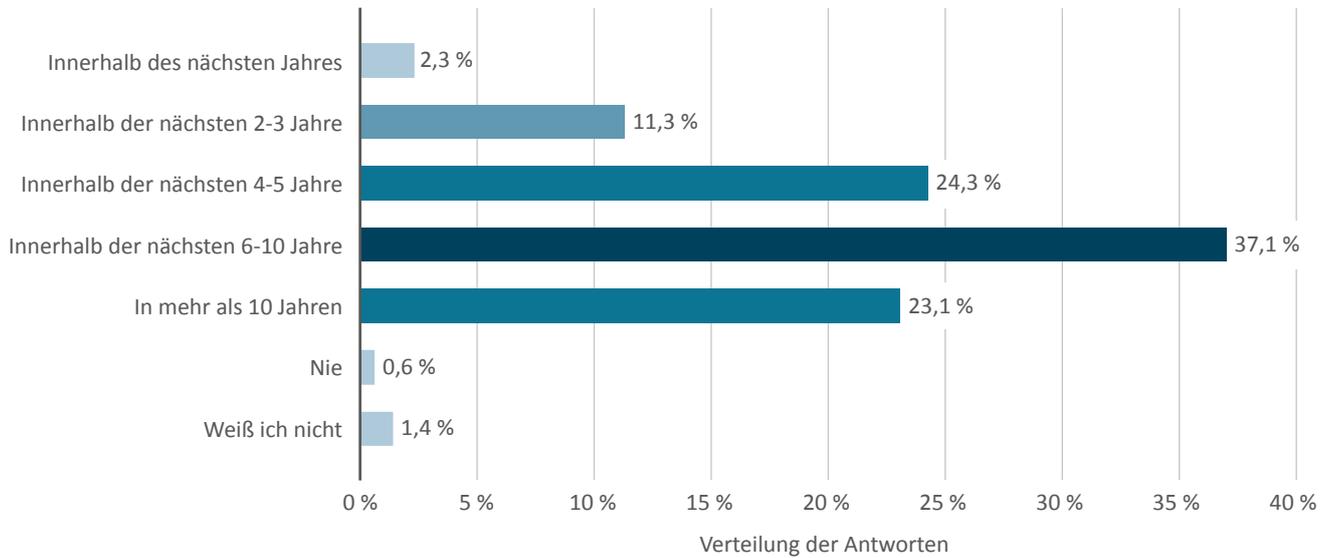
Es ist davon auszugehen, dass in den nächsten fünf bis zehn Jahren Quantencomputer mit mehreren tausend Qubits und geringer Fehlerrate verfügbar sein werden. Solche Systeme könnten kommerzielle Anwendungen in diversen Branchen ermöglichen und klassischen Supercomputern zunehmend überlegen sein. Neben der Hardware-Entwicklung wird auch an Software-Stacks und Programmierumgebungen für Quantencomputer gearbeitet, die die Anwendungsentwicklung vereinfachen.

Ein **Software-Stack** für Quantencomputer bezeichnet die Gesamtheit der Softwareebenen, die für die Programmierung und Steuerung eines Quantencomputers erforderlich sind – von der Hardware-nahen Steuerungssoftware bis zur Anwendungsebene. Die zentrale Aufgabe des Software-Stacks liegt in der Übersetzung komplexer Quantenalgorithmen in ausführbare Quantenoperationen sowie der Optimierung und Fehlerkorrektur dieser Operationen auf der physikalischen Ebene. Der Aufbau leistungsfähiger Software-Stacks gilt als entscheidender Erfolgsfaktor für die kommerzielle Nutzung von Quantencomputern und bindet erhebliche Entwicklungsressourcen der Technologieunternehmen.

Bis 2030 könnte ein **Quanten-Internet** entstehen, in dem Quantencomputer Berechnungen verteilt durchführen und über verschränkte Photonenkanäle kommunizieren. Dies sind hochspezialisierte optische Übertragungswege, die den Transport von Quanteninformation mittels einzelner Lichtteilchen ermöglichen. Diese Technologie bildet das Rückgrat der Quantenkommunikation, indem sie die präzise Übertragung von Quantenzuständen zwischen verschiedenen Quantenprozessoren oder Quantenspeichern gewährleistet.

Auch **Quantenkryptographie** wird an Bedeutung gewinnen. In 20 bis 30 Jahren könnten fehlertolerante universelle Quantencomputer mit Millionen von Qubits realisiert werden. Dann rücken transformative Anwendungen wie Quantensimulationen ganzer Zellen oder Materialien sowie Künstliche Intelligenz-Systeme auf Quantenrechnern in greifbare Nähe. Abb. 14 fasst den jeweils erwarteten Zeitpunkt der Überlegenheit von Quantencomputern gegenüber klassischen Computern für bestimmte Aufgaben zusammen.

Abb. 14: Erwartete Durchsetzungszeit für Quantencomputer



Quelle: QuEra Computing (2024, Umfrage)

7.3 Handlungsempfehlungen: Quantencomputing für Praktiker und Investoren



Die Quantenwelt eröffnet uns eine völlig neue Dimension der Informationsverarbeitung.

Hartmut Neven, Leiter des *Google Quantum Artificial Intelligence Lab*⁸⁶



Unternehmen sollten frühzeitig beginnen, Einsatzpotentiale von Quantencomputing für ihr Geschäft zu evaluieren.⁸⁷ Die Integration von Quantentechnologien erfordert von Unternehmen und Investoren eine systematische und strategische Herangehensweise. Die nachfolgenden Handlungsempfehlungen basieren auf der aktuellen Marktentwicklung und berücksichtigen sowohl technologische als auch wirtschaftliche Aspekte der Quantenrevolution.

Für Unternehmen der Realwirtschaft steht zunächst die strategische Vorbereitung im Vordergrund. Die Entwicklung einer dezidierten Quantenstrategie mit klar definierter Roadmap bis 2030 bildet das Fundament für alle weiteren Maßnahmen. Diese Strategie muss eine systematische

Analyse der Geschäftsprozesse auf Quantenpotentiale beinhalten und einen detaillierten Transformationsplan mit konkreten Meilensteinen und Budgets umfassen. Besonders wichtig ist die frühzeitige Identifikation kritischer Geschäftsprozesse, die sich für Quantenanwendungen eignen.

Die organisatorischen Maßnahmen konzentrieren sich auf den Aufbau effizienter Strukturen für die Quantentransformation. Die Einrichtung eines Quantenkompetenzzentrums als zentrale Koordinationsstelle hat sich dabei als besonders erfolgreich erwiesen. Dieses Zentrum koordiniert die Aktivitäten verschiedener Fachabteilungen und steuert den Kompetenzaufbau. Die Etablierung interdisziplinärer Teams aus Fach- und Technologieexperten sichert die erfolgreiche Umsetzung von Quantenprojekten. Eine klare Governance-Struktur gewährleistet die effektive Steuerung der Quanteninitiativen.

Der systematische Kompetenzaufbau stellt einen kritischen Erfolgsfaktor dar. Unternehmen müssen gezielt Quantenspezialisten und Fachinformatiker rekrutieren und gleichzeitig ihre Führungskräfte in Quantentechnologien schulen. Interne Weiterbildungsprogramme für Schlüsselmitarbeiter sichern die breite Verankerung des Quantenwissens in der Organisation. Kooperationen mit Hochschulen und Forschungseinrichtungen ermöglichen den Zugang zu aktuellem Fachwissen und qualifizierten Nachwuchskräften.

Im Finanzsektor ergeben sich spezifische Anforderungen an die technologische Anpassung. Die Implementierung quantensicherer Kryptographieverfahren hat höchste Priorität, um die Sicherheit von Finanztransaktionen auch in der Quantenära zu gewährleisten. Die Entwicklung hybrider Rechnerarchitekturen ermöglicht die schrittweise Integration von Quantenalgorithmien in bestehende Systeme. Die Modernisierung der Risikomanagementsysteme und der Aufbau quantenbasierter Handelsplattformen sind weitere zentrale Aufgaben.

Die Geschäftsentwicklung im Finanzsektor muss die Potentiale der Quantentechnologie systematisch erschließen. Dies umfasst die Konzeption quantenbasierter Finanzprodukte und die Entwicklung spezialisierter Beratungsangebote. Die Integration von Quantenalgorithmien in das Portfoliomanagement eröffnet neue Möglichkeiten der Optimierung und Risikosteuerung. Anlagestrategien müssen an die erweiterten Möglichkeiten der Quantencomputer angepasst werden.

Für strategische Investoren ergeben sich daraus unterschiedliche Investitionsschwerpunkte, konzentriert auf vier Kernbereiche: Quantenhardware mit Fokus auf etablierte Technologieunternehmen, Quantensoftware mit Ausrichtung auf Spezialanbieter, Quantenanwendungen mit Schwerpunkt auf Branchenführer in Schlüsselmärkten sowie Quanteninfrastruktur mit Fokus auf systemrelevante Technologieanbieter.

Die praktische Umsetzung dieser Überlegungen erfolgt in drei Phasen. Kurzfristig, innerhalb von ein bis zwei Jahren, stehen die Erstellung einer Quantenstrategie, der Aufbau erster Pilotprojekte, der Beginn des Kompetenzaufbaus und die Identifikation strategischer Partner im Vordergrund. Mittelfristig, in drei bis fünf Jahren, folgen die Skalierung erfolgreicher Pilotprojekte, der Ausbau der Quanteninfrastruktur, die Entwicklung quantenbasierter Produkte und die Vertiefung strategischer Partnerschaften. Längerfristig, nach 5+ Jahren, stehen die vollständige Integration von Quantentechnologien, die Erschließung neuer Geschäftsfelder, der Aufbau von Marktführerschaft in Schlüsselbereichen und die kontinuierliche Weiterentwicklung der Quantenstrategie im Fokus.

Der Erfolg dieser Transformation hängt maßgeblich von der konsequenten Umsetzung der Handlungsempfehlungen ab. Entscheidend sind dabei die frühzeitige strategische Positionierung, der systematische Aufbau von Kompetenzen und Ressourcen sowie die langfristige Perspektive bei der Umsetzung der Quantenstrategie. Unternehmen und Investoren, die diese Aspekte berücksichtigen, werden von den Chancen der Quantenrevolution deutlich profitieren können.

Erläuterungen

- 1 Auer et al. (2024, Quantencomputing im Finanzsystem).
- 2 Rometty, G. (2019, Quantenüberlegenheit).
- 3 BIS Innovation Hub (2024, Project Leap).
- 4 Feynman (1982, Simulation).
- 5 Jones (1998, Algorithmen).
- 6 Atom Computing (2023, Startup).
- 7 IBM (2024, IBM Roadmap).
- 8 Zeilinger (2005, Einsteins Schleier).
- 9 Zeilinger (2005, Einsteins Schleier).
- 10 Zempel et al. (2024, Quantum-Monitor).
- 11 Zempel et al. (2024, Quantum-Monitor).
- 12 Zempel et al. (2024, Quantum-Monitor).
- 13 Zempel et al. (2024, Quantum-Monitor).
- 14 Rigetti (2021, Quantenüberlegenheit).
- 15 Deutsch (2018, Quantenüberlegenheit).
- 16 Gambetta (2020, Skalierung).
- 17 Choi et al. (2023, Quantum Tortoise).
- 18 Krishna (2023, WEF 2023).
- 19 Verein für Computergenealogie e.V. – CompGen (2023, GenWiki).
- 20 Zempel et al. (2024, Quantum-Monitor).
- 21 Rebstrost/Lloyd (2024, Quantum Computational Finance).
- 22 Van Dam et al. (2024, Chemische Systeme).
- 23 Fraunhofer IIS (2024, Quantenchemie).
- 24 McKinsey & Company (2021, Use Cases).
- 25 Zempel et al. (2024, Quantum-Monitor).
- 26 QuEra Computing (2024, Umfrage).
- 27 Ladd et al. (2010, Einführung).
- 28 Nielsen/Chuang (2010, Quantum Computation).
- 29 Hidary (2019, Anwendung).
- 30 Lloyd (2011, Quantenmechanik).
- 31 Preskill (2018, Noisy Intermediate-Scale Quantum).
- 32 Orús et al. (2019, Finanzwirtschaft).
- 33 Arute et al. (2019, Quantenüberlegenheit).
- 34 Ladd et al. (2010, Einführung).
- 35 Montanaro (2016, Algorithmen).
- 36 Russo (2022, Vorausschauende Software).
- 37 Lidar/Brun (2013, Fehlerkorrektur).
- 38 Kruger (2022, Plattformen).
- 39 DiVincenzo (2000, Herausforderungen).
- 40 Rigetti (2021, Quantenüberlegenheit).
- 41 Smith-Goodson (2022, PsiQuantum).
- 42 Restelica (2024, Google).
- 43 Morvan et al. (2024, Phasenübergänge).
- 44 Morvan et al. (2024, Phasenübergänge).
- 45 Podbregar (2024, Quantinium).
- 46 Patsch (2024, Oxford Ionics).
- 47 Universität zu Köln (2024, Quantenmaterialien).
- 48 Trumpf (2023, Industrietauglichkeit).
- 49 Stauffer (2024, Nachbau von Quantenmodellen).
- 50 Mlynek (2017, Quantentechnologie).
- 51 DB Systel (2024, High Performance Computing).
- 52 Gil (2022, Ctech).
- 53 McKinsey & Company (2023, Transformation).
- 54 IBM (2023, Quantencomputer).
- 55 Isler (2024, Quantencomputing und Supply Chain Management).
- 56 Veritis (2024, Quantencomputing-Anwendungen).
- 57 Axmann (2023, Quantencomputing).
- 58 Joubert/Griedlich (2024, Grundlagen).
- 59 Shor (2021, Quantenkryptographie).
- 60 BSI (2024, Quantentechnologien); BSI (2024, Post-Quanten-Kryptografie).
- 61 Grover (1996, Algorithmik).
- 62 Kumar Rao et al. (2017, Kryptographie).
- 63 Van Meter et al. (2005, Architektur).
- 64 Shor (1994, Algorithmik).
- 65 Deodoro et al. (2021, Finanzwirtschaft).
- 66 NZZ (2023, Quantentechnologien).
- 67 Rapp (2024, Space).
- 68 Kharpal (2023, Quantum-Investitionen).
- 69 Fortune Business Insights (2024, Markt).
- 70 Fortune Business Insights (2024, Markt).
- 71 Fortune Business Insights (2024, Markt).
- 72 Fortune Business Insights (2024, Markt).
- 73 Langione et al. (2019, Risiken).
- 74 Lazzarotto (2024, Geopolitik).
- 75 The White House (2022, USA und Quantum).
- 76 Omaar/Makaryan (2024, China und Quantum).
- 77 Zempel et al. (2024, Quantum-Monitor).
- 78 European Commission (2022, Europa und Quantum).
- 79 Europäische Kommission (2023, Risikobewertung).
- 80 McKinsey & Company (2022, Ökosystem).
- 81 National Academies of Sciences, Engineering, and Medicine (2022, Fortschritte).
- 82 Nadella (2023, WEF 2023).
- 83 Zempel et al. (2024, Quantum-Monitor).
- 84 Zempel et al. (2024, Quantum-Monitor).
- 85 Zempel et al. (2024, Quantum-Monitor).
- 86 Neven (2024, Quantenüberlegenheit).
- 87 Ménard et al. (2020, Adaption).

Literaturverzeichnis

Bücher und Publikationen

- Arute, F. et al.** (2019, Quantenüberlegenheit): Quantum Supremacy Using a Programmable Superconducting Processor, *Nature* (Band 574, S. 505–510), veröffentlicht 23.10.2019, <https://www.nature.com/articles/s41586-019-1666-5>, zuletzt abgerufen am 13.10.2024.
- Auer, R./Dupont, A./Gambacorta, L./Park, J. S./Takahashi, K./Valko, A.** (2024, Quantencomputing im Finanzsystem): Quantum Computing and the Financial System: Opportunities and Risks, Bank for International Settlements, veröffentlicht 04.10.2024, <https://www.bis.org/publ/bppdf/bispap149.htm>, zuletzt abgerufen am 31.10.2024.
- Choi, S./Moses, W./Thompson, N.** (2023, Quantum Tortoise): The Quantum Tortoise and the Classical Hare: A Simple Framework for Understanding Which Problems Quantum Computing Will Accelerate (and Which It Will Not), Cornell University, veröffentlicht 24.10.2023, <https://arxiv.org/abs/2310.15505>, zuletzt abgerufen am 12.10.2024.
- DiVincenzo, D. P.** (2000, Herausforderungen): The Physical Implementation of Quantum Computation, *Fortschritte der Physik* (Band 48, S. 771–783), veröffentlicht 25.10.2000, <https://onlinelibrary.wiley.com/doi/abs/10.1002/1521-3978%28200009%2948%3A9%3C771%3A%3AAID-PROP771%3E3.0.CO%3B2-E>, zuletzt abgerufen am 17.07.2024.
- Feynman, R.** (1982, Simulation): Simulating Physics with Computers, *International Journal of Theoretical Physics*, veröffentlicht 06.1982, <https://doi.org/10.1007/BF02650179>, zuletzt abgerufen am 03.09.2024.
- Grover, L. K.** (1996, Algorithmik): A Fast Quantum Mechanical Algorithm for Database Search, *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (STOC '96)*, Association for Computing Machinery, veröffentlicht 01.07.1996, <https://doi.org/10.1145/237814.237866>, zuletzt abgerufen am 19.10.2024.
- Hidary, J.** (2019, Anwendung): Quantum Computing: An Applied Approach, Springer, veröffentlicht 25.09.2019, <https://link.springer.com/book/10.1007/978-3-030-23922-0>, zuletzt abgerufen am 13.10.2024.
- IBM** (2023, Quantencomputer): IBM Quantencomputer demonstriert den nächsten Schritt auf dem Weg jenseits des klassischen Supercomputings, veröffentlicht 15.06.2023, https://de.newsroom.ibm.com/2023-06-15_IBM-Quantencomputer-demonstriert-den-nachsten-Schritt?asPDF=1, zuletzt abgerufen am 02.11.2024.
- Kumar Rao, S./Mahto, D./Yadav, D. K.** (2017, Kryptographie): The AES-256 Cryptosystem Resists Quantum Attacks, *International Journal of Advanced Research in Computer Science*, veröffentlicht 30.04.2017, <https://doi.org/10.26483/ijarcs.v8i3.3025>, zuletzt abgerufen am 03.07.2024.
- Ladd, T. D. et al.** (2010, Einführung): Quantum Computers, *Nature* (Band 464, S. 45–53), veröffentlicht 04.03.2010, https://www.researchgate.net/publication/41761089_Quantum_computers, zuletzt abgerufen am 27.09.2024.
- Lidar, D./Brun, T.** (2013, Fehlerkorrektur): Quantum Error Correction, Cambridge University Press, veröffentlicht 12.09.2013, <https://www.lehmanns.ch/shop/naturwissenschaften/25289531-9780521897877-quantum-error-correction>, zuletzt abgerufen am 19.08.2024.
- Montanaro, A.** (2016, Algorithmen): Quantum Algorithms: An Overview, *npj Quantum Information*, veröffentlicht 12.01.2016, <https://www.nature.com/articles/npjqi201523>, zuletzt abgerufen am 14.08.2024.
- Morvan, A. et al.** (2024, Phasenübergänge): Phase Transitions in Random Circuit Sampling, *Nature*, veröffentlicht 09.10.2024, <https://www.nature.com/articles/s41586-024-07998-6>, zuletzt abgerufen am 31.10.2024.
- National Academies of Sciences, Engineering, and Medicine** (2022, Fortschritte): Quantum Computing: Progress and Prospects, The National Academies Press, veröffentlicht in 2022, <https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects>, zuletzt abgerufen am 18.10.2024.
- Nielsen, M./Chuang, I.** (2010, Quantum Computation): Quantum Computation and Quantum Information, Cambridge University Press, veröffentlicht 11.12.2010, <https://www.cambridge.org/core/books/quantum-computation-and-quantum-information/01E10196D0A682A6AEFFEA52D53BE9AE>, zuletzt abgerufen am 07.10.2024.
- Orús, R. et al.** (2019, Finanzwirtschaft): Quantum Computing for Finance: Overview and Prospects, *Reviews in Physics*, veröffentlicht 28.06.2019, <https://www.sciencedirect.com/science/article/pii/S2405428318300571>, zuletzt abgerufen am 13.10.2024.
- Petric, R., Sorge, C., Ziebarth, W.** (2022, Datenschutz): Datenschutz: Einführung in technischen Datenschutz, *Datenschutzrecht und angewandte Kryptographie*, Springer Vieweg Wiesbaden, veröffentlicht 02.01.2022, <https://link.springer.com/book/10.1007/978-3-658-39097-6#page=34>, zuletzt abgerufen am 17.07.2024.
- Pfeiffer, R./Lampert, J./Hoefnagels, J.** (2021, Quantum Computing): Die Zukunft des Quantum Computings – Die zweite Quantenrevolution, veröffentlicht 01.2021, <https://2bahead.com/downloads/zukunftsstudie-zukunft-des-quantum-computings>, zuletzt abgerufen am 04.11.2024.
- Preskill, J.** (2018, Noisy Intermediate-Scale Quantum): Quantum Computing in the NISQ Era and beyond, *Quantum*, veröffentlicht 06.08.2018, <https://quantum-journal.org/papers/q-2018-08-06-79/>, zuletzt abgerufen am 04.10.2024.
- QuEra Computing** (2024, Umfrage): The Current and Future State of Quantum Computing, *QuEra Computing*, veröffentlicht 07.2024, https://uploads-ssl.webflow.com/643b94c382e84463a9e52264/66add72e0b8354a8451d9305_QuEra%20July%202024%20Survey%20Report.pdf, zuletzt abgerufen am 11.08.2024.
- Rapp, H.-W./von Bartenwerffer, T.** (2019, Quantencomputer): Quantencomputer, Internet of Things und superschnelle Kommunikationsnetze: Die Treiber der Disruption in künstlicher Intelligenz und Digitalisierung, veröffentlicht bei FERI Cognitive Finance Institute, erschienen am 11.2019, https://www.feri.ch/media/vpwp0ks/fcfc_5g-201911.pdf, zuletzt abgerufen am 21.10.2024.
- Rapp, H.-W.** (2021, Great Progression): The Great Progression: Das Jahrzehnt massiver Beschleunigung, veröffentlicht bei FERI Cognitive Finance Institute, erschienen am 03.2021, https://www.feri.ch/media/1nxbgwbl/fcfc_greatprogression-202103-kurzversion.pdf, zuletzt abgerufen am 21.10.2024.
- Rapp, H.-W.** (2023, KI): KI: The Next Level – Die transformative Wucht des Megatrends „Künstliche Intelligenz“, veröffentlicht bei FERI Cognitive Finance Institute, erschienen am 23.08.2023, https://www.feri-institut.de/media/pwnlseuu/202308_ki_the-next-level.pdf, zuletzt abgerufen am 04.11.2024.
- Rapp, H.-W.** (2024, Space Cold War): „Space Cold War“ – Massive Militarisierung des Weltraums als globales Risiko, veröffentlicht bei FERI Cognitive Finance Institute, erschienen am 27.06.2024, https://www.feri-institut.de/media/eudl4obq/feri_cf_cc_space_2406120.pdf, zuletzt abgerufen am 04.11.2024.
- Rebentrost, P./Lloyd, S.** (2024, Quantum Computational Finance): Quantum Algorithm for Portfolio Optimization, Springer, veröffentlicht 12.08.2024, <https://link.springer.com/article/10.1007/s13218-024-00870-9>, zuletzt abgerufen am 02.11.2024.
- Rigetti, C.** (2021, Quantenüberlegenheit): How Quantum Computing Will Change Everything (with Chad Rigetti), HBR, veröffentlicht 15.12.2021, <https://hbr.org/podcast/2021/12/how-quantum-computing-will-change-everything-with-chad-rigetti>, zuletzt abgerufen am 30.10.2024.
- Shor, P.** (1994, Algorithmik): Algorithms for Quantum Computation: Discrete Logarithms and Factoring, IEEE Computer Society Press, veröffentlicht 22.11.1994, <https://ieeexplore.ieee.org/document/365700>, zuletzt abgerufen am 17.09.2024.

- Van Dam, W. et al.** (2024, Chemische Systeme): End-to-End Quantum Simulation of a Chemical System, arXiv, veröffentlicht 09.09.2024, <https://arxiv.org/abs/2409.05835>, zuletzt abgerufen am 02.11.2024.
- Van Meter, R./Itoh, K. M./Ladd, T. D.** (2005, Architektur): Architecture-Dependent Execution Time of Shor's Algorithm, Proc. Mesoscopic Superconductivity, veröffentlicht 04.07.2005, <https://arxiv.org/abs/quant-ph/0507023>, zuletzt abgerufen am 17.07.2024.
- Zeilinger, A.** (2005, Einsteins Schleier): Einsteins Schleier: Die neue Welt der Quantenphysik, C. H. Beck, veröffentlicht 15.09.2005, <https://www.perlentaucher.de/buch/anton-zeilinger/einsteins-schleier.html>, zuletzt abgerufen am 13.10.2024.
- Zemmel, R. et al.** (2024, Quantum-Monitor): Steady Progress in Approaching Quantum Advantage, McKinsey Digital, veröffentlicht 24.04.2024, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/steady-progress-in-approaching-the-quantum-advantage>, zuletzt abgerufen am 30.10.2024.

Zeitungen und Internetquellen

- Atom Computing** (2023, Startup): Quantum Startup Atom Computing First to Exceed 1,000 Qubits, Atom Computing, veröffentlicht 24.10.2023, <https://www.prnewswire.com/news-releases/quantum-startup-atom-computing-first-to-exceed-1-000-qubits-301964712.html>, zuletzt abgerufen am 17.07.2024.
- Axmann, R.** (2023, Quantencomputing): Leiter der Quantencomputing-Initiative des Deutschen Zentrums für Luft- und Raumfahrt (DLR), zitiert nach: Hamburg News, veröffentlicht 20.06.2023, <https://hamburg-business.com/de/news/quantencomputing-3-vielversprechende-anwendungsfelder>, zuletzt abgerufen am 04.11.2024.
- BIS Innovation Hub** (2024, Project Leap): Project Leap: Quantum-Proofing the Financial System, Bank for International Settlements, veröffentlicht 11.01.2024, https://www.bis.org/about/bisih/topics/cyber_security/leap.htm, zuletzt abgerufen am 30.10.2024.
- BSI Bundesamt für Sicherheit in der Informationstechnik** (2024, Quantentechnologien): Quantentechnologien und quantensichere Kryptografie, veröffentlicht 2024, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-quantensichere-kryptografie_node.html, zuletzt abgerufen am 05.11.2024.
- BSI Bundesamt für Sicherheit in der Informationstechnik** (2024, Post-Quanten-Kryptografie): Post-Quanten-Kryptografie, veröffentlicht 2024, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/Post-Quanten-Kryptografie_node.html, zuletzt abgerufen am 05.11.2024.
- DB Systel** (2024, High Performance Computing): High Performance und Quanten Computing – Wie Quantencomputer die Zukunft der Bahn prägen können, veröffentlicht 2024, <https://www.dbsystel.de/dbsystel/Consulting-und-Innovation/Quantencomputing-9108998>, zuletzt abgerufen am 02.11.2024.
- Deodoro, J./Gorbanyov, M./Malaiika, M./Sedik, T. S.** (2021, Finanzwirtschaft): Quantum Computing and the Financial System: Spooky Action at a Distance?, International Monetary Fund, veröffentlicht 21.03.2021, <https://www.imf.org/en/Publications/WP/Issues/2021/03/12/Quantum-Computing-and-the-Financial-System-Spooky-Action-at-a-Distance-50159>, zuletzt abgerufen am 04.09.2024.
- Deutsch, D.** (2018, Quantenüberlegenheit): David Deutsch on the Infinite Reach of Knowledge, TED, veröffentlicht 10.2018, https://www.ted.com/talks/the_ted_interview_david_deutsch_on_the_infinite_reach_of_knowledge?subtitle=en, zuletzt abgerufen am 30.10.2024.
- Egger, D. et al.** (2020, Quantum Computing for Finance): Quantum Computing for Finance: State-of-the-Art and Future Prospects, IEEE Transactions on Quantum Engineering, veröffentlicht 24.06.2020, <https://ieeexplore.ieee.org/document/9222275>, zuletzt abgerufen am 13.06.2024.
- European Commission** (2022, Europa und Quantum): Quantum Technologies Flagship, European Commission, aktualisiert 2022, <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>, zuletzt abgerufen am 18.10.2024.
- Europäische Kommission** (2023, Risikobewertung): EU-Kommission empfiehlt Risikobewertungen für vier kritische Technologiebereiche, veröffentlicht 04.10.2023, https://germany.representation.ec.europa.eu/news/eu-kommission-empfehlrt-risikobewertungen-fur-vier-kritische-technologiebereiche-2023-10-04_de, zuletzt abgerufen am 08.11.2024.
- Fortune Business Insights** (2024, Markt): Quantum Computing Market Size 2024-2032, Fortune Business Insights, veröffentlicht 30.09.2024, <https://www.fortunebusinessinsights.com/quantum-computing-market-104855>, zuletzt abgerufen am 04.10.2024.
- Fraunhofer IIS** (2024, Quantenchemie): Quantencomputer Meets Quantenchemie: KI-gestützte Verfahren verbessern Molekülforschung, veröffentlicht 12.03.2024, https://www.iis.fraunhofer.de/de/pr/2024/20240312_quantencomputer_meets_quantenchemie.html, zuletzt abgerufen am 02.11.2024.
- Gambetta, J.** (2020, Skalierung): IBM's Roadmap for Scaling Quantum Technology, veröffentlicht 15.09.2020, <https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/>, zuletzt abgerufen am 26.07.2024.
- Gil, D.** (2022, Ctech): Quantum Leap: The Big Bang of Quantum Computing Will Come in this Decade, Ctech, veröffentlicht 18.10.2022, <https://www.calcalistech.com/ctechnews/article/b1kbb9fqj>, zuletzt abgerufen am 30.10.2024.
- Hansen, L. W.** (2024, Quanteninvestition): Why Invest in Quantum Computing? Ask the Box at Alice & Bob, Alice & Bob, veröffentlicht 01.2024, <https://alice-bob.com/blog/why-invest-in-quantum-computing-ask-the-box-at-alice-bob/>, zuletzt abgerufen am 30.10.2024.
- IBM** (2024, IBM Roadmap): IBM Quantum: Development & Innovation Roadmap, IBM, veröffentlicht 2024, https://www.ibm.com/quantum/assets/IBM_Quantum_Development_&_Innovation_Roadmap.pdf, zuletzt abgerufen am 29.08.2024.
- Isler, K.** (2024, Quantencomputing und Supply Chain Management): Quantencomputing und Supply Chain Management: Neue Wege für Geschäftsführer, HageIT, veröffentlicht 29.10.2024, <https://www.hageit.de/it-insights/quantencomputing-und-supply-chain-management-neue-wege-fuer-geschaeftsfuehrer.html>, zuletzt abgerufen am 02.11.2024.
- Jones, J. A.** (1998, Algorithmen): Implementation of a Quantum Algorithm on a Nuclear Magnetic Resonance Quantum Computer, American Institute of Physics, veröffentlicht 01.08.1998, <https://qudev.phys.ethz.ch/static/content/courses/QSIT09/pdfs/Jones1998.pdf>, zuletzt abgerufen am 04.07.2024.
- Joubert, A./Griedlich, N.** (2024, Grundlagen): Quantum Computing: Unlocking the Unknown, Deloitte Luxembourg, veröffentlicht 2024, <https://www.deloitte.com/lu/en/Industries/technology/blogs/quantum-computing.html>, zuletzt abgerufen am 19.10.2024.
- Kharpal, A.** (2023, Quantum-Investitionen): Investing in Quantum Computing: A Guide, NASDAQ, veröffentlicht 14.04.2023, <https://www.nasdaq.com/articles/investing-in-quantum-computing--a-guide>, zuletzt abgerufen am 03.07.2024.
- Krishna, A.** (2023, WEF 2023): Chairman & CEO of IBM Arvind Krishna Explains Company's Quantum Computing Achievements @ Davos 2023, World Economic Forum, veröffentlicht 02.02.2023, <https://thequantuminsider.com/2023/02/02/chairman-ceo-of-ibm-arvind-krishna-explains-companys-quantum-computing-achievements-davos-2023/>, zuletzt abgerufen am 30.10.2024.
- Kruger, P.** (2022, Plattformen): Quantum Computing Hardware & Software: Industry Overview, veröffentlicht 18.11.2022, PsiQuantum, <https://www.psiquantum.com/blog/quantum-computing-hardware-software>, zuletzt abgerufen am 26.07.2024.
- Langione, M. et al** (2019, Risiken): Where Will Quantum Computers Create Value — and When?, Boston Consulting Group, veröffentlicht 13.05.2019, <https://www.bcg.com/publications/2019/quantum-computers-create-value-when>, zuletzt abgerufen am 26.07.2024.
- Lazzarotto, Y. V.** (2024, Geopolitik): Comparative Analysis of Quantum Technology Policies: China, European Union, and United States, Graduate Institute of International and Development Studies, veröffentlicht im 09.2024, <https://www.graduateinstitute.ch/sites/internet/files/2024-09/Final-Report-4--Yiannos-Vittorio-Lazzarotto.pdf>, zuletzt abgerufen am 30.09.2024.

- Lloyd, S.** (2011, Quantenmechanik): Quantencomputer sind der Schlüssel zur Entschlüsselung der Geheimnisse des Universums, NOVA, veröffentlicht 21.07.2011, <https://www.pbs.org/wgbh/nova/article/quantum-computing/>, zuletzt abgerufen am 30.10.2024.
- McKinsey & Company** (2021, Use Cases): Quantum Computing Use Cases Are Getting Real — What You Need to Know, veröffentlicht 14.12.2021, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know>, zuletzt abgerufen am 26.07.2024.
- McKinsey & Company** (2022, Ökosystem): Quantum Computing: An Emerging Ecosystem and Industry Use Cases, McKinsey & Company, veröffentlicht 14.12.2022, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-use-cases-are-getting-real-what-you-need-to-know>, abgerufen am 03.10.2024.
- McKinsey & Company** (2023, Transformation): Europäische Autoindustrie in größter Transformation ihrer Geschichte, veröffentlicht 30.08.2023, <https://www.mckinsey.com/de/news/presse/2023-30-08-automotive-masterplan>, zuletzt abgerufen am 02.11.2024.
- Ménard, A./Ostojic, I./Patel, M./Volz, D.** (2020, Adaption): A Game Plan for Quantum Computing, McKinsey & Company, veröffentlicht 06.02.2020, <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/a-game-plan-for-quantum-computing>, zuletzt abgerufen am 21.10.2024.
- Mlynek, J.** (2017, Quantentechnologie): Q&A: How UK Partners Can Participate in the EU Quantum Technologies Flagship Programme, Imperial College London, veröffentlicht 09.06.2017, <https://nqit.ox.ac.uk/video/qa-how-uk-partners-can-participate-eu-quantum-technologies-flagship-programme.html>, zuletzt abgerufen am 30.10.2024.
- Nadella, S.** (2023, WEF 2023): Davos 2023: A Conversation with Satya Nadella, World Economic Forum, veröffentlicht 18.01.2023, <https://www.weforum.org/podcasts/agenda-dialogues/episodes/davos-2023-a-conversation-with-satya-nadella/>, zuletzt abgerufen am 30.10.2024.
- Neven, H.** (2024, Quantenüberlegenheit): Quantum Computers Aren't What You Think — They're Cooler, TED, veröffentlicht 14.04.2024, https://www.ted.com/talks/hartmut_neven_quantum_computers_aren_t_what_you_think_they_re_cooler?subtitle=en, zuletzt abgerufen am 30.10.2024.
- NZZ** (2023, Quantentechnologien): China erforscht mit hohem Tempo Quantentechnologien fürs Militär. Die USA und die Nato sind besorgt, veröffentlicht 30.01.2023, <https://www.nzz.ch/technologie/quanten-technologien-fuers-militaer-chinas-tempo-beschaefigt-usa-ld.1722745>, zuletzt abgerufen am 04.11.2024.
- Omaar, H./Makaryan, M.** (2024, China und Quantum): How Innovative Is China in Quantum?, Information Technology and Innovation Foundation, veröffentlicht 09.09.2024, <https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/>, zuletzt abgerufen am 27.08.2024.
- Patsch, S.** (2024, Oxford Ionics): Quantenchip von Oxford Ionics bricht Performance-Rekord, Heise Online, veröffentlicht 16.07.2024, <https://www.heise.de/news/Oxford-Ionics-entwickelt-leistungstaerksten-Quantenchip-9802615.html>, zuletzt abgerufen am 26.07.2024.
- Podbregar, N.** (2024, Quantinuum): Quantencomputer knackt Rekord – 56-Qubit-Rechner beweist Quanten-Überlegenheit mit bisher geringster Fehlerquote, Scinexx, veröffentlicht 15.07.2024, <https://www.scinexx.de/news/technik/quantencomputer-knackt-rekord/>, zuletzt abgerufen am 26.07.2024.
- Quantinuum** (2024, System Model H2): Quantinuum System Model H2: 56 Qubits Challenging the World's Best Supercomputers, veröffentlicht 05.06.2024, <https://www.youtube.com/watch?v=mnGtDb5qHs&t=9s>, zuletzt abgerufen am 04.11.2024.
- Restelica, E.** (2024, Google): This Thing is NOT an Alien! – Is Google's Quantum Computer!, veröffentlicht 26.07.2024, https://www.linkedin.com/posts/endritrestelica_technology-ai-google-activity-7209872701929250816-xaGf, zuletzt abgerufen am 26.07.2024.
- Rometty, G.** (2019, Quantenüberlegenheit): IBM CEO Rometty Says Quantum Will Solve Problems Traditional Computers Can't, Bloomberg, veröffentlicht 19.09.2019, <https://www.bloomberg.com/news/videos/2019-09-18/rometty-says-quantum-will-solve-problems-traditional-computers-can-t-video>, zuletzt abgerufen am 30.10.2024.
- Russo, S.** (2022, Vorausschauende Software): Vorausschauende Software beschleunigt das Training von neuronalen Netzen, ETH Zürich, veröffentlicht 18.01.2022, <https://ethz.ch/de/news-und-veranstaltungen/eth-news/news/2022/01/eine-vorausschauende-software-beschleunigt-das-training-von-neuronalen-netzen.html>, zuletzt abgerufen am 02.11.2024.
- Shor, P.** (2021, Quantenkryptographie): Interview with Peter Shor, EP News, veröffentlicht 10.03.2021, <https://ep-news.web.cern.ch/content/interview-peter-shor>, zuletzt abgerufen am 30.10.2024.
- Smith-Goodson, P.** (2022, PsiQuantum): PsiQuantum Has a Goal for Its Million Qubit Photonic Quantum Computer to Outperform Every Supercomputer on the Planet, Forbes, veröffentlicht 21.09.2022, <https://www.forbes.com/sites/moorinsights/2022/09/21/psiquantum-has-a-goal-for-its-million-qubit-photonic-quantum-computer-to-outperform-every-supercomputer-on-the-planet/>, zuletzt abgerufen am 17.10.2024.
- Stauffer, P.** (2024, Nachbau von Quantenmodellen): Ein Schritt näher zu Quantentechnologien: Fundamentales Quantenmodell exakt nachgebaut, Eidgenössisches Departement für Wirtschaft, Bildung und Forschung WBF, veröffentlicht 31.10.2024, <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-102928.html>, zuletzt abgerufen am 31.10.2024.
- Thaker, A./Adam, S.** (2018, Branchen): The Coming Quantum Leap in Computing, Boston Consulting Group, veröffentlicht 16.05.2018, <https://www.bcg.com/publications/2018/coming-quantum-leap-computing>, zuletzt abgerufen am 26.07.2024.
- The White House** (2022, USA und Quantum): President Biden Announces Two Presidential Directives Advancing Quantum Technologies, The White House, veröffentlicht 04.05.2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/>, zuletzt abgerufen am 11.08.2024.
- Trumpf** (2023, Industrietauglichkeit): Trumpf macht Quantencomputer industrietauglich, Trumpf, veröffentlicht 17.10.2023, https://www.trumpf.com/de_CH/newsroom/stories/trumpf-macht-quantencomputer-industrietauglich/, zuletzt abgerufen am 14.10.2024.
- Universität zu Köln** (2024, Quantenmaterialien): Durchbruch an der Kante: Forschende schaffen wichtige Voraussetzung für Quantencomputer, veröffentlicht 10.07.2024, <https://portal.uni-koeln.de/universitaet/aktuell/presseinformationen/detail/durchbruch-an-der-kante-forschende-schaffen-wichtige-voraussetzung-fuer-quantencomputer>, zuletzt abgerufen am 26.07.2024.
- Verein für Computergenealogie e.V. – CompGen** (2023, GenWiki): DNA – GenWiki, veröffentlicht 2023, <https://wiki.genealogy.net/DNA>, zuletzt abgerufen am 02.11.2024.
- Veritis** (2024, Quantencomputing-Anwendungen): Top Applications of Quantum Computing, veröffentlicht 2024, <https://www.veritis.com/blog/top-applications-of-quantum-computing/>, zuletzt abgerufen am 02.11.2024.

Impressum

Herausgeber: FERI Cognitive Finance Institute, Bad Homburg

Autor: Dr. Michael Blaschke, Global Principal IT Architect, Experte für Institutional DLT, Unternehmensberater für Technologiestrategie, Podcast Co-Host „Bitcoin, Fiat & Rock'n'Roll“

Veröffentlichung: November 2024

Bisherige Analysen und Publikationen im FERI Cognitive Finance Institute:

Studien:



1. Carbon Bubble und Dekarbonisierung (2017)
2. Overt Monetary Finance (OMF) (2017)
3. Die Rückkehr des Populismus (2017)
4. KI-Revolution in der Asset & Wealth Management Branche (2017)
5. Zukunftsrisiko „Euro Break Up“ (2018)
6. Die Transformation zu einer kohlenstoffarmen Wirtschaft, (2018)
7. Wird China zur Hightech-Supermacht? (2018)
8. Zukunftsrisiko „Euro Break Up“, 2. aktualisierte und erweiterte Auflage (2018)
9. Risikofaktor USA (2018)
10. Impact Investing: Konzept, Spannungsfelder und Zukunftsperspektiven (2019)
11. „Modern Monetary Theory“ und „OMF“ (2019)
12. Alternative Mobilität (2019)
13. Digitalisierung – Demographie – Disparität (2020)
14. „The Great Divide“ (2020)
15. Zukunftstrend „Alternative Food“ (2020)
16. Digitalisierung – Demographie – Disparität, 2. aktualisierte und erweiterte Auflage (2020)
17. „The Great Progression“ (2021)
18. „Blockchain und Tokenisierung“ (2021)
19. „The Monetary Supercycle“ (2021)
20. Wasserstoff als Energiequelle der Zukunft (2022)
21. Sustainable Blue Economy (2022)
22. Chinas globales Powerplay (2022)
23. Quo vadis, Europa? (2023)
24. Neue Weltordnung – „Made in China“ (2023)
25. Vorteil Biodiversität – Lösungsansätze und Investitionschancen im Einklang mit der Natur (2024)
26. Globale Rezession der Freiheit (2024)
27. Die BioTech-Revolution – Neue Dynamik durch innovative Technologien (2024)

Cognitive Comments:



1. Network Based Financial Markets Analysis (2017)
2. Zwischen Populismus und Geopolitik (2017)
3. „Neue Weltordnung 2.0“ (2017)
4. Kryptowährung, Cybermoney, Blockchain (2018)
5. Dekarbonisierungsstrategien für Investoren (2018)
6. Innovation in blockchain-based business models and applications in the enterprise environment (2018)
7. Künstliche Intelligenz, Quanten-Computer und Internet of Things - Die kommende Disruption der Digitalisierung (2019)
8. Quantencomputer, Internet of Things und superschnelle Kommunikationsnetze (2019)
9. Was bedeutet die CoVid19-Krise für die Zukunft? (2020)
10. Trouble Spot Taiwan – ein gefährlich unterschätztes Problem (2021)
11. Urban Air Mobility – Flugdrohnen als Transportmittel der Zukunft (2021)
12. „Longevity“: Megatrend Langlebigkeit – Die komplexen Auswirkungen und Konsequenzen steigender Lebenserwartung (2022)
13. Hightech-Metalle und Seltene Erden – Akute Rohstoff-Risiken für Europas Zukunft (2022)
14. Amerika auf dem Weg zur Autokratie – Anatomie und Perspektiven einer gespaltenen Großmacht (2022)
15. Vertical Farming – Technologische Innovation zur Umgestaltung des globalen Ernährungssystems (2023)
16. Generation Z – Potentiale der jungen Generation für globale Disruption (2023)
17. KI: The Next Level – Die transformative Wucht des Megatrends „Künstliche Intelligenz“ (2023)
18. Chinas Angriff auf den US-Dollar – Maßnahmen, Motive und mögliche Risiken für das westliche Finanzsystem (2023)
19. „Trump reloaded“ – Drohender Umbau der USA in eine Präsidialdiktatur (2024)
20. 3D-Druck und Additive Fertigung: Unterschätztes Potential zur Transformation wichtiger Zukunftstrends (2024)
21. Takeoff der Tokenisierung – 2024 als Katalysatorjahr der Token-Ökonomie (2024)
22. „Space Cold War“: Massive Militarisierung des Weltraums als globales Risiko (2024)
23. Quantenzeitalter – Quantencomputing als Gamechanger für Finanz- und Realwirtschaft (2024)

Cognitive Briefings:



1. Ressourcenverbrauch der Digital-Ökonomie (2020)
2. Globale Bifurkation oder „New Cold War“? (2020)
3. Digitaler Euro: Das Wettrennen zwischen Europäischer Zentralbank und Libra* Association (2020)
4. Herausforderung „Deep Fake“ (2021)
5. Geoökonomische Zeitenwende (2022)
6. Brennpunkt Taiwan (2023)
7. CRISPR/Cas (2023)
8. „New Space“ (2024)

Diese und noch viele weitere themenspezifische Veröffentlichungen haben wir auf unserer Webseite hinterlegt: www.feri-institut.de



FERI AG | FERI Cognitive Finance Institute
Das strategische Forschungszentrum der FERI Gruppe
Haus am Park
Rathausplatz 8 – 10
61348 Bad Homburg v.d.H.
Tel. +49 (0)6172 916-3631
info@feri-institut.de
www.feri-institut.de



Rechtliche Hinweise: Alle Angaben und Quellen werden sorgfältig recherchiert. Für Vollständigkeit und Richtigkeit der dargestellten Information wird keine Gewähr übernommen. Diese Publikation ist urheberrechtlich geschützt. Jede weitere Verwendung, insbesondere der gesamte oder auszugsweise Nachdruck oder die nicht nur private Weitergabe an Dritte, ist nur mit vorheriger schriftlicher Zustimmung von FERI gestattet. Die nicht autorisierte Einstellung auf öffentlichen Internetseiten, Portalen oder anderen sozialen Medien ist ebenfalls untersagt und kann rechtliche Konsequenzen nach sich ziehen. Die angeführten Meinungen sind aktuelle Meinungen, mit Stand des in diesen Unterlagen aufgeführten Datums. FERI AG, Stand 2024