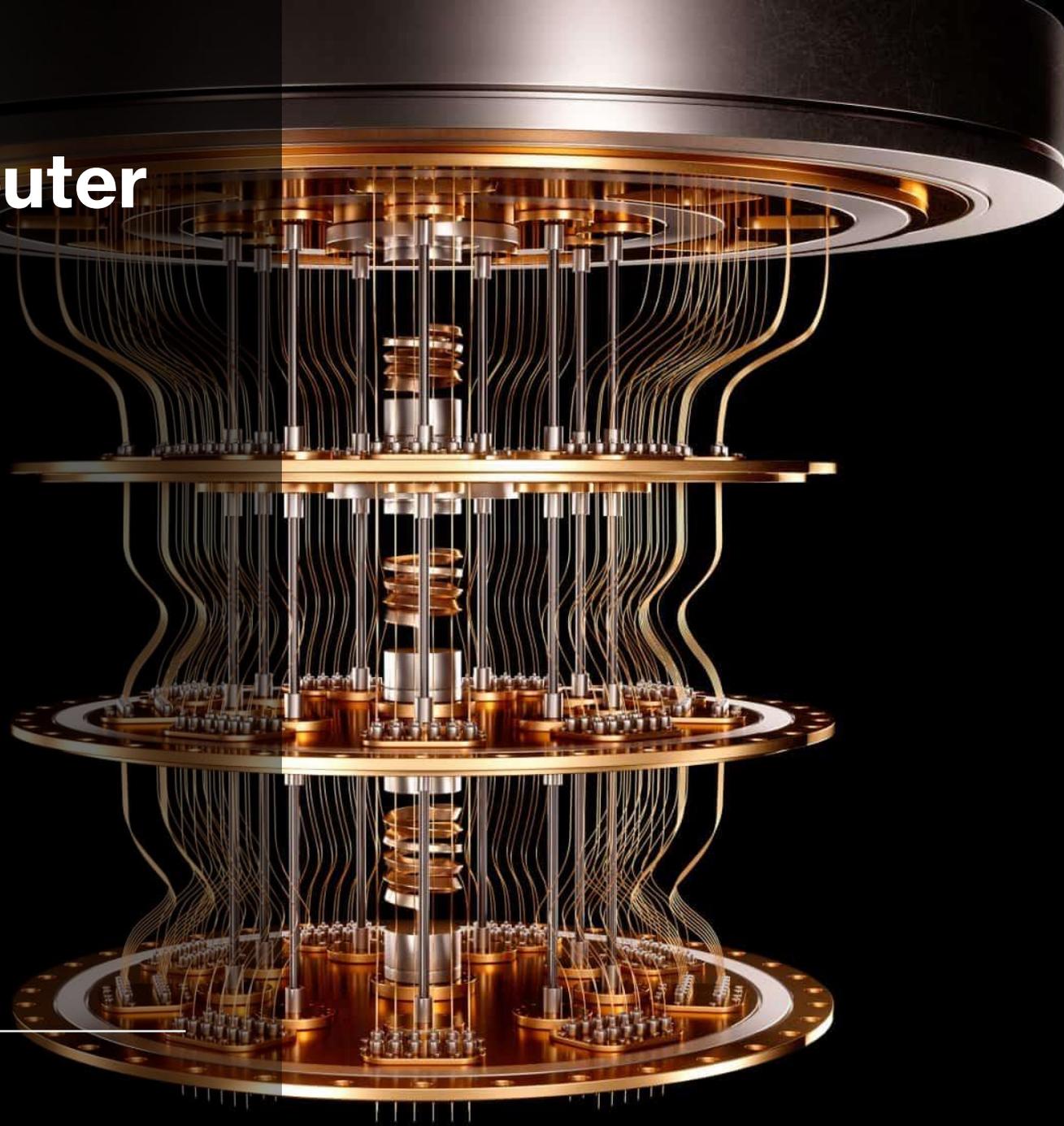
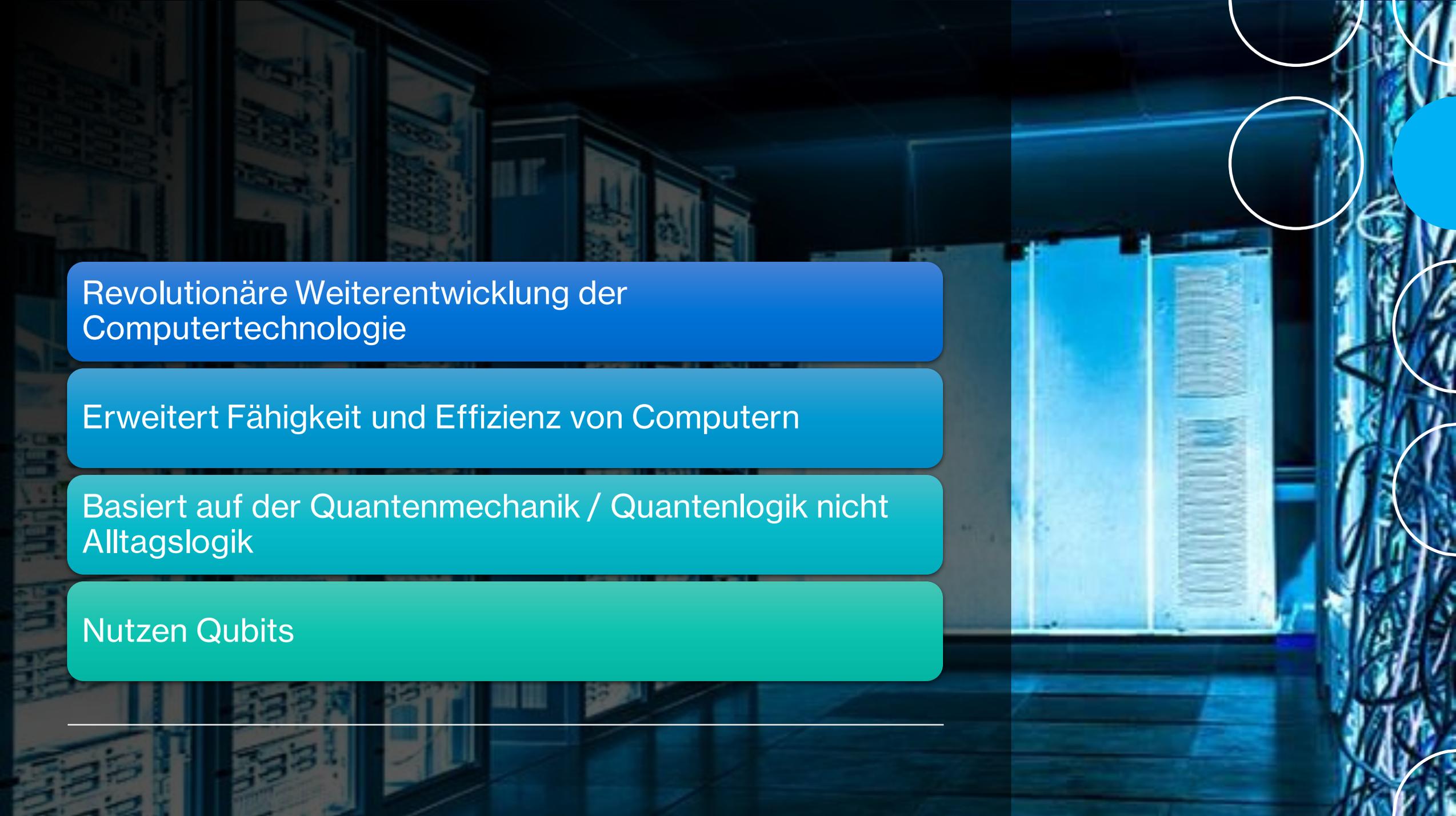


Quantencomputer

Ferdinand K.
Jonathan D.
Stefan E.





Revolutionäre Weiterentwicklung der Computertechnologie

Erweitert Fähigkeit und Effizienz von Computern

Basiert auf der Quantenmechanik / Quantenlogik nicht Alltagslogik

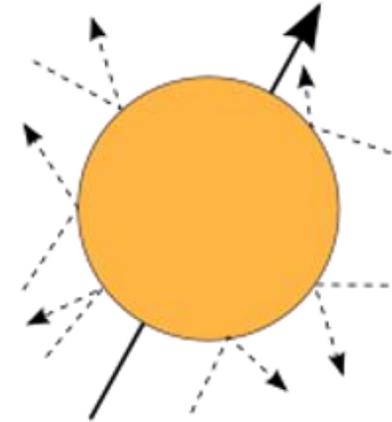
Nutzen Qubits

Aspekt	Herkömmlicher Computer	Quantencomputer
Grundlage	Basiert auf klassischer Logik	Nutzt Quanten-Logik
Recheneinheiten	Bits	Qubits
Zustände der Einheiten	Nur 0 oder 1	Beliebige Überlagerung zwischen 0 und 1
Schaltungselemente	Logische Gatte (Nicht, Oder, Und)	Quantengatter (H, X, Y, Z, CNOT)
Potenzialsteigerung	Linearer Anstieg mit Rechenleistung	Exponentielle Steigerung mit jedem Qubit
Aktuelle Größe	Groß, mit Millionen bis Milliarden Bits	Klein, mit 10 bis 65 Qubits
Programmierung	Herkömmliche Programme nutzbar	Erfordert neue Quanten-Algorithmen
Geschwindigkeitsvorteil	Begrenzt bei einigen Anwendungen	Potenziell massiver Vorteil bei spezifischen Anwendungen (z.B. Shor-Algorithmus)
Limitierungen	-	Rauschen begrenzt
Simulation	Simulierbar von Supercomputern	Ab etwa 50 Qubits nicht mehr simulierbar

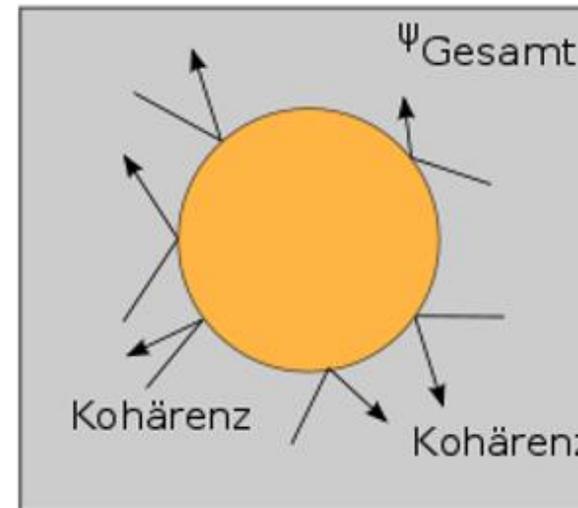
Quantenmechanik

- Teil der Physik, der das Verhalten von Teilchen auf atomarer und subatomarer Ebene beschreibt
- Teilchen hat mehrere Zustände gleichzeitig

a) klassisch

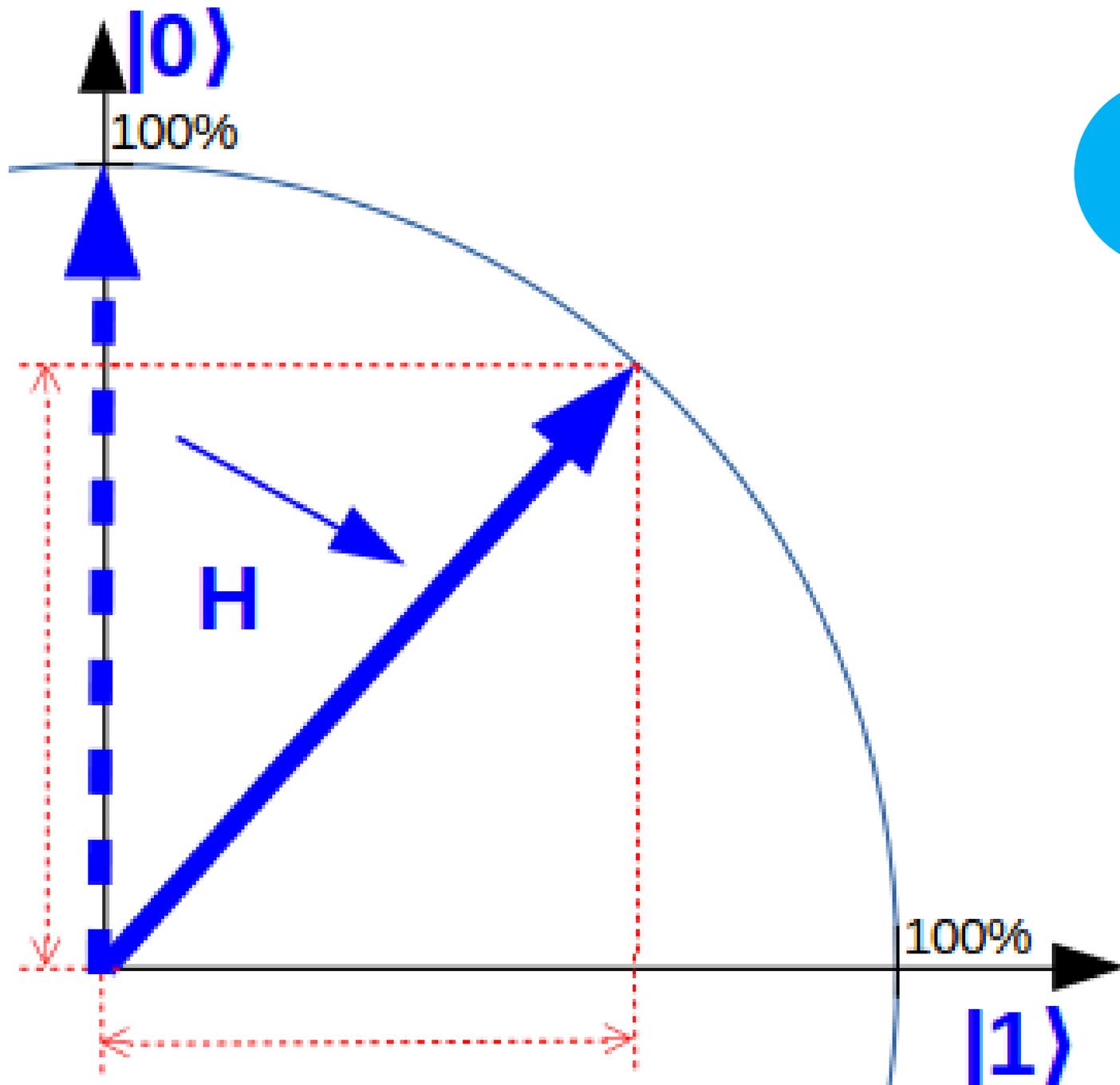


b) quantenmechanisch

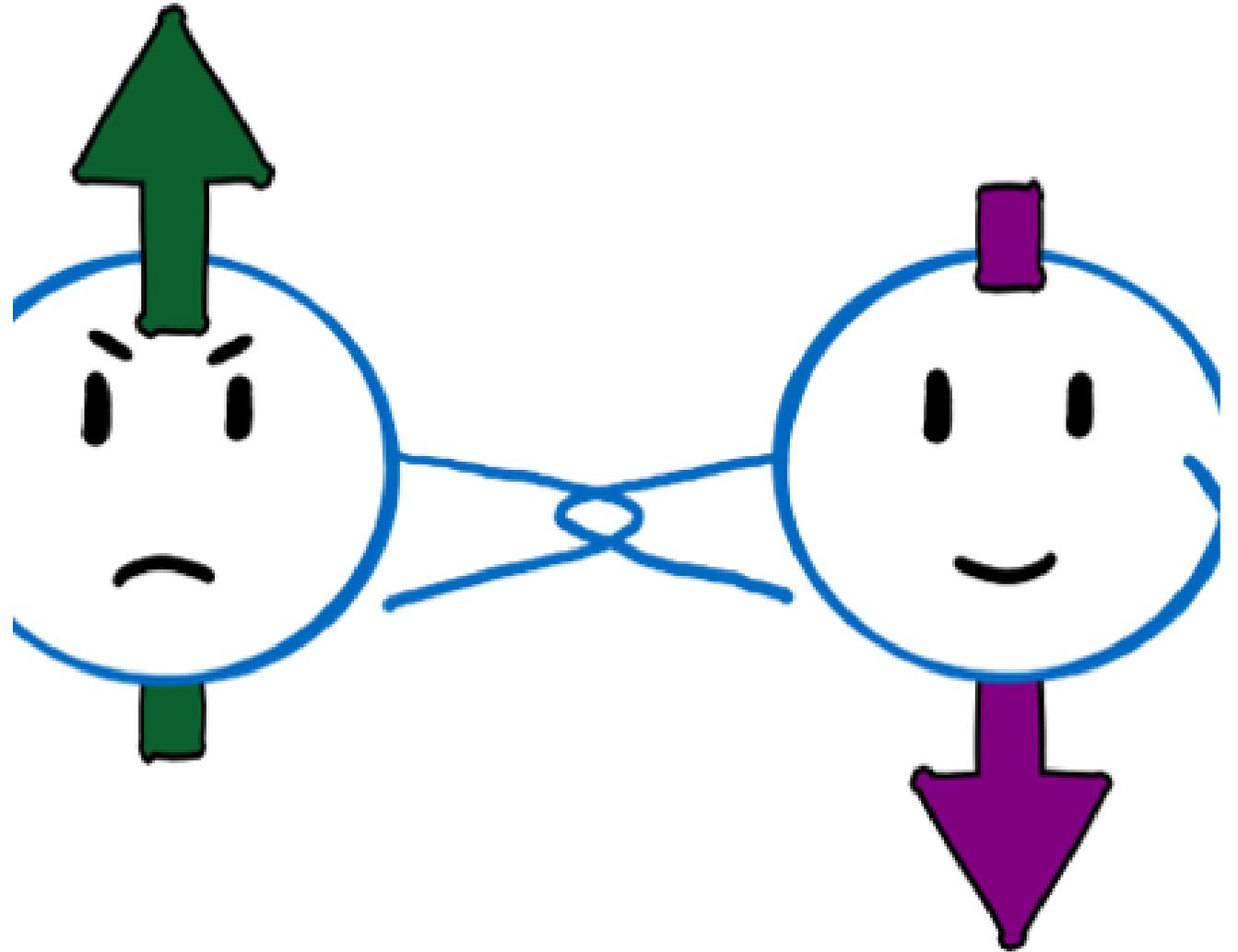


Was sind Qubits?

- Das Qubit kann, im Gegensatz zum klassischen Bit, das nur zwei Zustände annehmen kann (0 oder 1), mehrere Zustände gleichzeitig annehmen.
- Wird daher als Superposition bezeichnet



Qubits können **verschränkt** sein, was bedeutet, dass Änderungen an einem Qubit sofort **Änderungen** an anderen Qubits verursachen, unabhängig von der Entfernung.



Anwendung

Automobilindustrie (Robotikoptimierung
Verkehrsoptimierung
Pilotprojekte bei BMW und Volkswagen)

Pharmaindustrie (Beschleunigung der Wirkstoffsuche
Präzise Molekülsimulationen
Potenzielle Krebstherapieoptimierung

**Materialwissenschaft und
Energie** (Batterieentwicklung,
Innovative Materialentwicklung
)

**Meteorologie und
Klimaforschung:** Genauere
Vorhersagen, Klimawandel)

**Künstliche Intelligenz und
maschinelles Lernen**
(Mustererkennung, KI-Systeme)

Big Data-Verarbeitung (
DatenbankanalyseBeschleunigte
Verarbeitung)

Was ist eine Superposition?

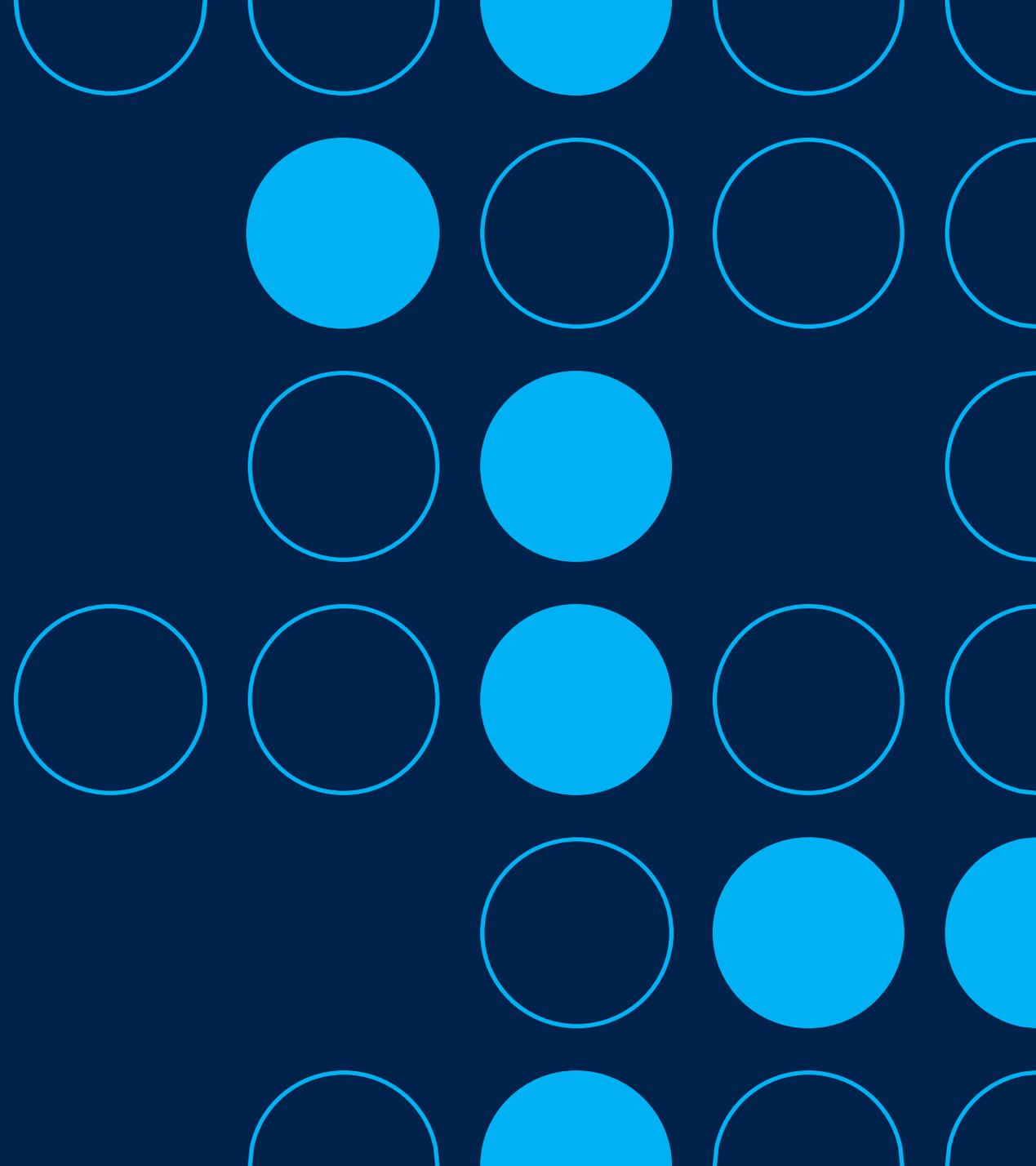
ein Konzept in der Quantenmechanik,
das besagt, dass Teilchen in mehreren
Zuständen gleichzeitig existieren
können, solange sie nicht beobachtet
oder gemessen werden



Schrödingers Katze

Warum verwenden Quantencomputer Superpositionen

Es ermöglicht die Durchführung
mehrerer paralleler Berechnungen
deren Ergebnis erst beim Messen
feststeht



Shor Algorithmus

1994 hatte er die Idee

Sein Algorithmus kam heraus bevor es überhaupt Quantencomputer gab

Er macht sich die Schwächen in dem RSA Crypto System zu Nutze:

Es gibt nur eine Lösung

Shors Algorithmus nutzt die Parallelität und Überlagerungseigenschaften von Quantencomputern, um das Faktorisierungsproblem effizienter zu lösen als klassische Algorithmen. Im Wesentlichen kann Shors Algorithmus in Polynomialzeit (genauer gesagt in $O((\log N)^3)$) faktorisieren, während die besten bekannten klassischen Algorithmen in sub-exponentieller Zeit (exponentiell langsamer als jede Polynomzeit) arbeiten.

Was ist Polynomialzeit

- In der Informatik bezieht sich der Begriff "**Polynomialzeit**" auf die **Laufzeitkomplexität** eines Algorithmus in Bezug auf die Größe des Eingabegegenstands. Ein Algorithmus wird als "Polynomialzeit" eingestuft, wenn seine Laufzeit durch ein Polynom in der Größe der Eingabe beschrieben werden kann.
 - Formell gesprochen ist ein **Algorithmus** in Polynomialzeit, wenn seine Laufzeit $T(n)$ durch eine Funktion $f(n)$ begrenzt wird, wobei $f(n)$ ein Polynom ist. **Mathematisch ausgedrückt:**
 - $T(n) = O(f(n))$
 - Hier steht $T(n)$ für die Laufzeit des Algorithmus in **Abhängigkeit** von der **Größe** der Eingabe n , und $f(n)$ ist ein Polynom. Die Exponenten des Polynoms bestimmen die Ordnung der Polynomialzeit.
-



Warum verwenden Quantencomputer Superpositionen

- Es ermöglicht die Durchführung mehrerer paralleler Berechnungen deren Ergebnis erst beim Messen feststeht



Google und die Quantencomputer



Gründung des Quantum AI Lab und D-Wave-Exploration

- Quantum AI Lab 2013 gegründet
- Leitung durch Hartmut Neven
- Ursprüngliches Ziel: Nutzung der D-Wave-Quanten-Hardware



Entscheidung für Eigenentwicklung eines Quantencomputers

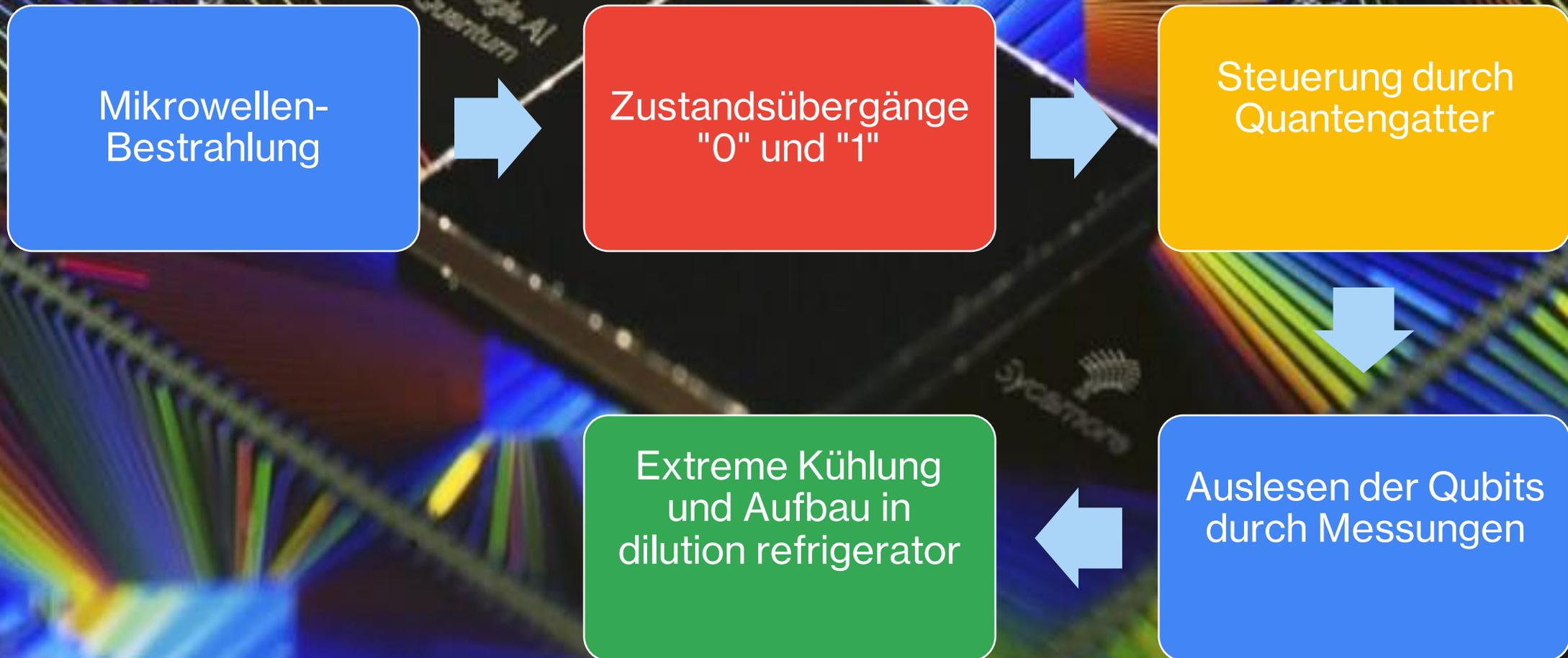
- Einschränkungen des D-Wave-Systems
- Google beschließt eigenen universellen Quantencomputer zu bauen



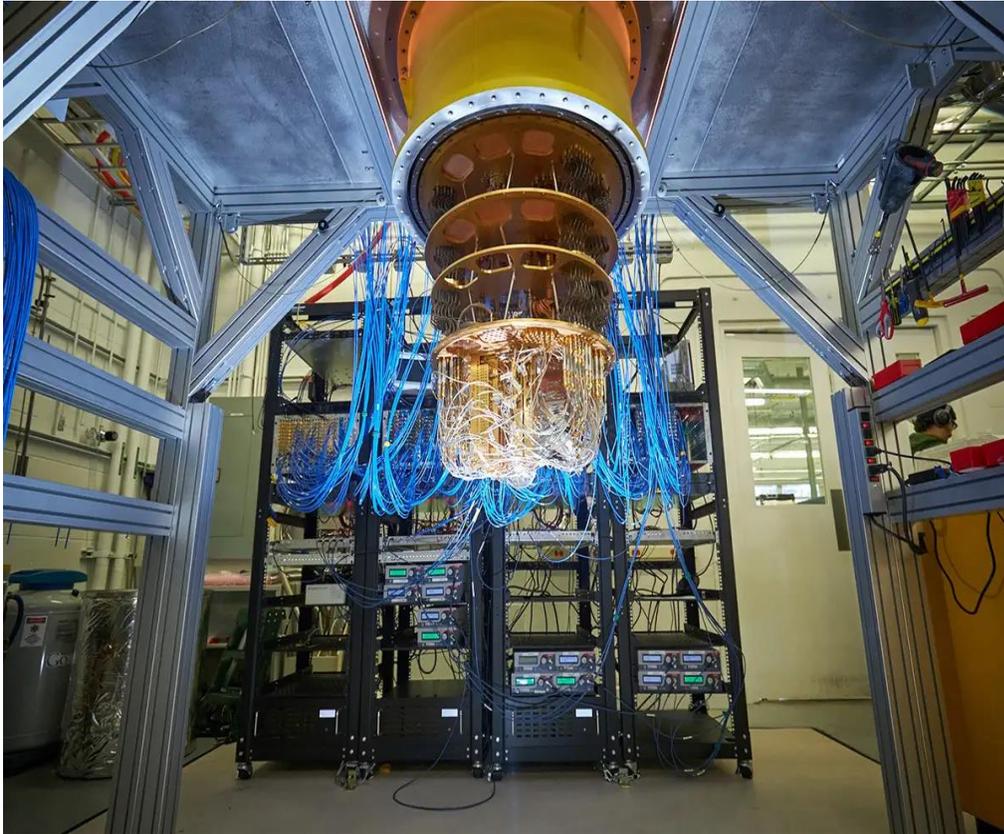
Erforschung der Supraleiter-Technologie mit John Martinis

- Start der Kooperation 2014 mit Physiker John Martinis
- Fokus auf Circuit QED und Schaffung von supraleitenden Qubits durch gezielte Lücken (Josephson Junctions)

Google und die Quantencomputer



Google und die Quantencomputer



Sycamore, ein 53-Qubit-Quantencomputer von Google, löste 2019 eine Aufgabe in Sekunden, die normale Supercomputer in 10.000 Jahren bewältigt hätten. Das zeigte die enormen Möglichkeiten von Quantencomputern für spezifische Aufgaben. Seine planare Qubit-Anordnung war bahnbrechend für zukünftige Entwicklungen. Die Erforschung fehlerkorrigierter Qubits wie dem Surface Code ist entscheidend für die Überwindung der NISQ-Ära.

Vorteile von Quantencomputer

Verschlüsselung im Bankwesen

- Überlegenheit bei komplexen Problemlösungen
- Schnelle Lösungen für Verschlüsselungsprozesse

Medizin und Forschung

- Simulation von Molekülen
- Potenzial für medizinische Forschung und Innovation

Big Data-Analyse

- Auswertungen großer Datenmengen
- Potenzielle Anwendungen



Nachteile

Spezialisierte Fachkenntnisse erforderlich (Notwendigkeit qualifizierter Fachkräfte)

Erfordert spezifisches Know-how zur Handhabung

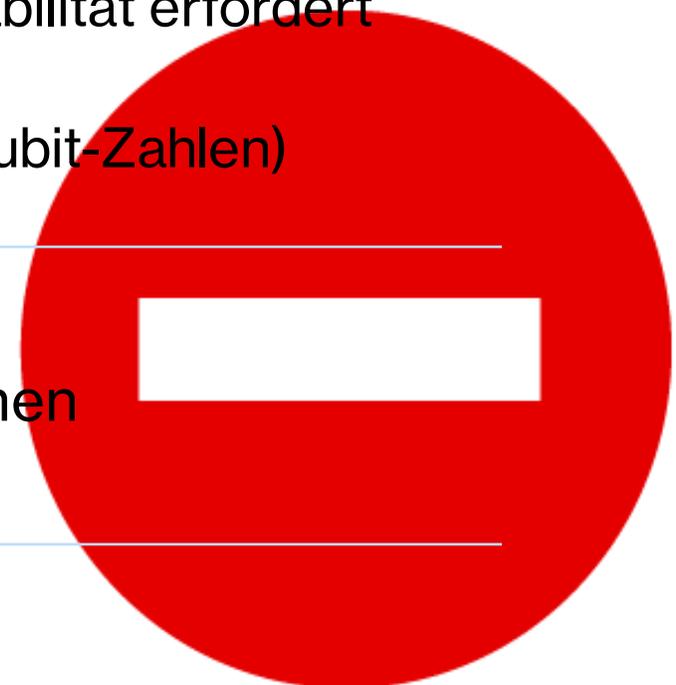
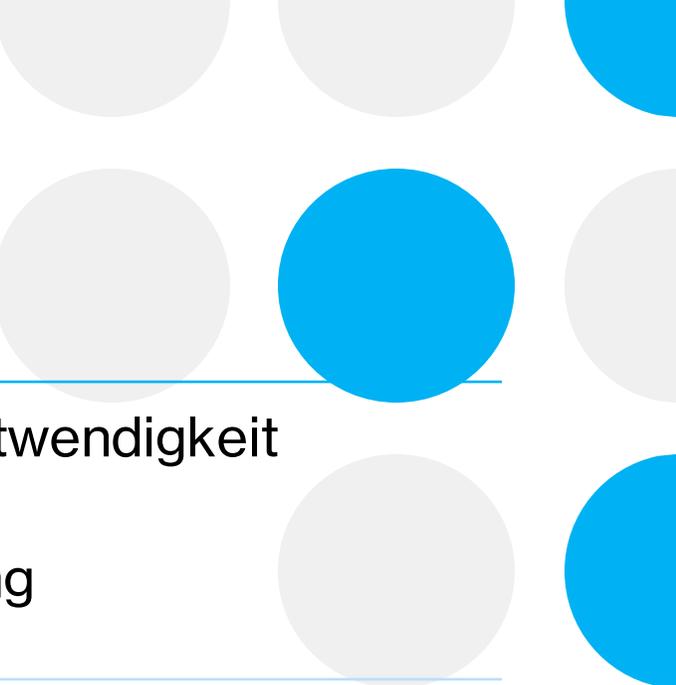
Stabilität durch Verschränkung von Qubits (Stabilität erfordert viele verschränkte Qubits)

Herausforderungen bei der Verwaltung großer Qubit-Zahlen)

Empfindlichkeit und Umweltbedingungen

Empfindlichkeit bei Temperatur und Vibrationen

Betrieb nahe dem absoluten Nullpunkt



Beschleunigte wissenschaftlicher
Forschung und Entwicklung neuer
Technologien

Verbesserte Datenanalyse und -
verarbeitung

*Mögliche
Zukunftsaussichten*

Optimierte von Verkehrs- und
Logistiksystemen

Großer Fortschritt in
der Kryptographie und
Cybersicherheit