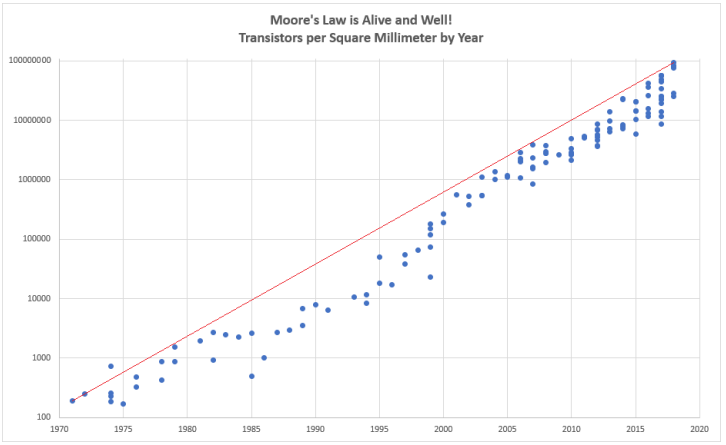
Quantencomputer

Herkömmliche Computer:



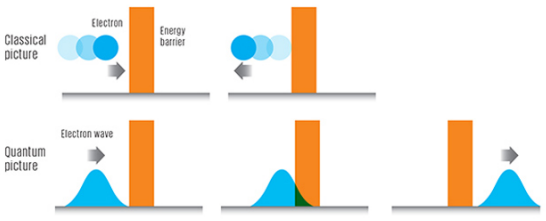
- Schon seit beginn stetige Weiterentwicklung von Computern, sie wurden leistungsfähiger und komplexer: z.B. Modernes Handy ist 120 Millionen mal so leistungsfähig, wie Apollo (erste Mondlandung) Computer
- 1965 hat Gordon Moore das mooresche Gesetz aufgestellt: er sagte voraus, dass sich alle 2 Jahre die Leistung von Computern verdoppelt

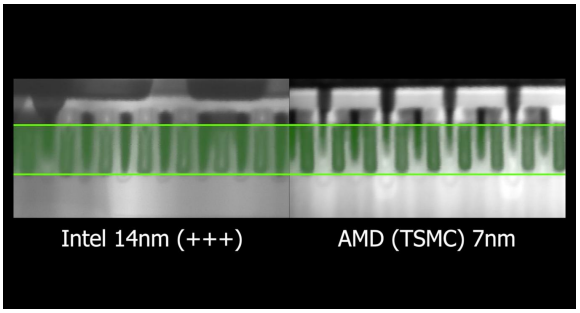
→ ist bis jetzt auch eingetreten

- Funktionsweise:
  - Daten werden als Bits gespeichert, die entweder 0 oder 1 sein können
  - Bits sind Transistoren, die wie elektronische Schalter funktionieren, wenn Strom fließen kann, dann 1, wenn nicht dann 0
  - Bits können zu Logikgattern kombiniert werden (z.B. AND-Logikgatter überprüft ob mehrere Bits 1 sind)
  - Logikgatter werden für komplexere Schaltungen benutzt (z.B. Addition)

→ Es werden sehr viele Transistoren für einfache Berechnungen, wie z.B. Addition verwendet

- Transistoren werden also immer kleiner, Bei sehr kleinen Größen tritt der Quantentunneleffekt auf, bei diesen “teleportieren” sich Elektronen durch Materie, da sie eine Wahrscheinlichkeitskurve haben, auf der sie überall auftauchen können, wenn diese Kurve größer als Materie ist können sie sich “teleportieren”
- Ab welcher größe der Quantentunneleffekt auftaucht ist vom Stoff abhängig, für Transistoren wird so gut wie immer Silizium verwendet
- Heutige kommerzielle Transistoren sind in etwa 14 bis 7 nm groß, bei 5 nm dritt dann der Quantentunneleffekt auf, jedoch ist es Forschern gelungen 1nm große Transistoren herzustellen, da sie einen sehr schweren Stoff genommen haben.



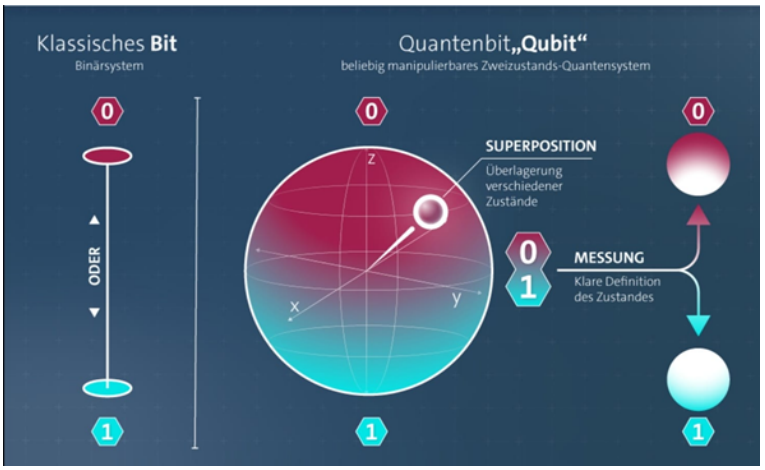


- Auch wenn man in der Masse 1nm große Transistoren bauen könnte, kommen die Transistoren irgendwann an die Grenze, wo sie die minimale Anzahl an Atome haben und von da an können Transistoren nicht kleiner werden

- Computer werden immer komplexer
- Kleinste Bauteile kommen an physikalische Grenze
- In einigen Jahren kann man herkömmliche Computer nicht mehr Leistungsfähiger machen

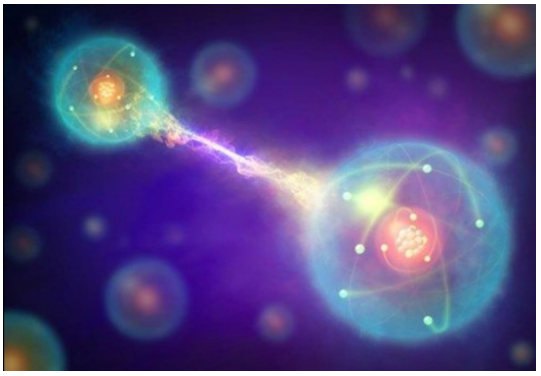
Funktionsweise:

- Arbeiten auf Basis quantenmechanischer Zustände (nicht auf Basis der Gesetze der klassischen Physik)
- Vorteile davon sind Möglichkeiten der Nutzung des Superpositionsprinzips und der Quantenverschränkung
- Grundlegender Unterschied zu normalen PCs: Nutzung von Qubits statt Bits
- Bits können als Informationsdarstellung nur einen von zwei Zuständen annehmen
- Qubits (kurz für Quanten-Bits) sind Quantensysteme und können quantenmechanische Zustände annehmen



- Besitzen keinen eindeutigen, bzw. jeden beliebigen Zustand (also alles von 0 bis 1) und nehmen nur einen eindeutigen Zustand an, wenn sie gemessen werden (Superpositionsprinzip)
- Bei Messung wird Zustand als einer von zweien definiert (z.B.durch Unterscheidung des Spins oder des Energieniveaus bei Elektronen)
- Durchführung mehrerer Rechnungen gleichzeitig möglich
- Mit genügend Qubits können bei komplexen Aufgaben gleichzeitig alle Möglichkeiten durchprobiert werden (normale Computer müssen eine nach der anderen abarbeiten)
- Superpositionen werden bei Nutzung von mehr Qubits effektiver -> Rechnungsvermögen steigt nicht linear, sondern exponentiell
- n Qubits entsprechen in Speicherkraft und Rechenleistung 2 hoch n Bits
- Quantencomputer mit 250 Qubits könnte mehr Zustände berechnen und speichern, als es Atome im Universum gibt
- dadurch könnte gesamtes Universum simuliert perfekter Schachcomputer gebaut werden

- wenn sich Qubits in Superposition befinden, können zwei oder mehr von diesen quantenmechanisch gekoppelt werden, sodass ihr Zustand voneinander abhängig ist; sie zählen trotz räumlicher Trennung als 1 Teilchen (Quantenverschränkung)



- wird nun Zustand eines Qubits festgelegt/gemessen, nimmt gekoppeltes Qubit in **Echtzeit** (also unmittelbar) den der Verschränkung entsprechenden Zustand (z.B. den gleichen oder entgegengesetzten) an
- durch Messungen verlassen Qubits Superposition und Quantenverschränkung wird aufgelöst
- Durch Quantenverschränkung ergibt sich die Möglichkeit, Qubits zu Schaltkreisen zusammenzuschließen

- Nutzung von Quantensystemen, sogenannten Qubits
- können Superpositionsprinzip und Quantenverschränkung nutzen
- Superpositionsprinzip: Qubits befinden sich nur bei Messung in einem eindeutigen Zustand, dadurch sind mehrere Rechnungen gleichzeitig möglich
- Quantenverschränkung

Geschichte:

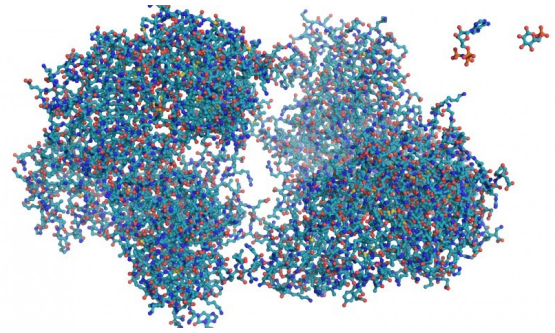
- Idee der Nutzung von Quantengesetzen in moderner Informatik entstand in 1980er Jahren
- Mitte der 1990er Jahre: Realisierung erster funktionierender Quantencomputer mit wenigen Qubits
- 2005: erste Erzeugung eines Quantenregisters mit 8 Qubits (Beweis benötigte 650000 Messungen und 10 Stunden)
- 2011: Entdeckung der Quantenverschränkung durch Mikrowellen (großer Schritt in Richtung effizientere Quantenverschränkung, trotz Erfolgschance von nur 76%)
- 2015: Eröffnung des ersten online-zugreifbaren Quantenprozessors durch IBM (auf Website konnten auch Programme für Quantencomputer geschrieben werden)
- 2018: bahnbrechender Quantencomputer von Google mit 72 funktionsfähigen Qubits und ziemlich niedriger Fehlerrate
- zeitgleich Entwicklung eines Simulators durch Microsoft, mit dem Quantencomputer auf normalen Rechnern simuliert werden konnten (schnelleres Auffinden von Fehlern und deren Ursachen in Quantencomputern möglich)
- Quantenüberlegenheit (Bezeichnung für Überlegenheit von Quanten- gegenüber normalen Computern) wurde im Oktober 2019 von Google-Forschern erstmals

eindrucksvoll demonstriert, indem ihr Quantenprozessor *Sycamore* mit 53 Qubits eine komplexe Berechnung in ca. 200 Sekunden durchführte, für die der modernste Supercomputer 10000 Jahre gebraucht hätte
- ähnliche Behauptung gab Gruppe chinesischer Wissenschaftler im Dezember 2020 ab (Prozessor hatte angeblich Problem in 200 Sekunden gelöst, für das Supercomputer 2,5 Milliarden Jahre benötigt hätten)
- In beiden Fällen wurden Ergebnisse von Konkurrenten angezweifelt und Aufgaben gelöst, die auf Quantenprozessoren zugeschnitten waren

- Beginn der Forschung in den 90er Jahren
- anschließend exponentielle Steigerung der Forschungsgeschwindigkeit (v.a. ab 2010)
- Konkurrenz zwischen zahlreichen Firmen beschleunigt Entwicklung zusätzlich
- große Durchbrüche ab 2015
- 100-Qubit-Grenze wurde überschritten, hohe Fehlerquote sorgt aber weiterhin für Probleme in der Effektivität

Zukunft:

- Quantencomputer sind in speziellen Anwendungen heute schon viel schneller als herkömmliche Computer, jedoch sind sie nicht universell einsetzbar
- wenn aber universell einsetzbar, sind sie allen normalen Computern überlegen
- Experten gehen davon aus, dass in zehn Jahren einsetzbare Quantencomputer existieren
- Die Voraussetzungen für Quantencomputern sind jedoch noch so hoch, dass wir wohl in naher Zukunft keine Quantencomputer zu hause nutzen können, da sie z.B. Temperaturen nahe 0°K benötigen
- Nutzen von Quantencomputer:
    - Datenbanken können viel schneller Durchsucht werden
    - Durch die parallelen Berechnungen können große Simulationen durchführen
    - komplexe Moleküle (z.B. Proteine) können simuliert werden, dadurch könnten bessere Medikamente oder neue Behandlungsmethoden simuliert und getestet werden
    - Ein zentraler Quantencomputer für alle Menschen, der teure Hardware zu hause ersetzt



- Nachteile und Gefahren:
    - Es lassen sich Verschlüsselungen in nur wenigen Sekunden knacken, bei denen herkömmliche Computer ewigkeiten brauchen würden

→ Es wird schon an Quanten Sicheren Verschlüsselungen gearbeitet, wobei man noch nicht genau weiß was alles Quantencomputer Sicher ist
    - Dadurch können sensible Daten, wie z.B. Bankdaten und Bankzugänge gehackt werden
    - Die Kryptowährungen, wie Bitcoin sind auch durch Algorithmen verschlüsselt, die in wenigen Sekunden von Quantencomputern gehackt werden können (einige Kryptowährungen geben aber selber an das sie Quantensicher sind: z.B. Cardano)
    - Regierungen und Firmen können durch Quantencomputer extrem Große Datenmengen über uns zu verwalten (noch extremer als eh schon)
    - Es ist nicht klar, wie weit die Forschung, vor allem bei Regierungen wirklich ist, mit den Regierungen ist es nicht so unwahrscheinlich, Edward Snowden (Whistleblower der NSA) sagte bereits 2014, dass die NSA an Quantencomputern arbeitet

- noch nicht universell einsetzbar
- kann vor allem zur Krankheitsbekämpfung (Simulation) und zur Datenbankverarbeitung genutzt werden
- Verschlüsselungen können sehr einfach gehackt werden, und es ist unklar wie weit Quantencomputern schon in der Entwicklung sind