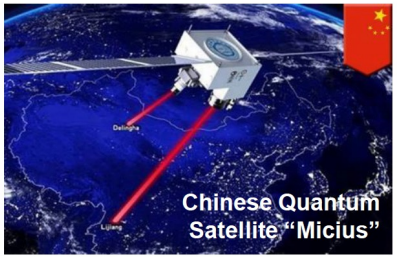
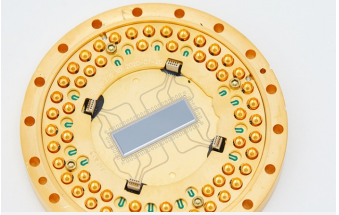
Die zweite Quantenrevolution: Sind Quantenrechner die Zukunft des Computing?

Peter P. Orth (Universität des Saarlandes)

Tag der offenen Tür, Universität des Saarlandes, 8. Juni 2024





Quantum Processing Unit (QPU) von Rigetti Computing

Quanteninformationstechnologien

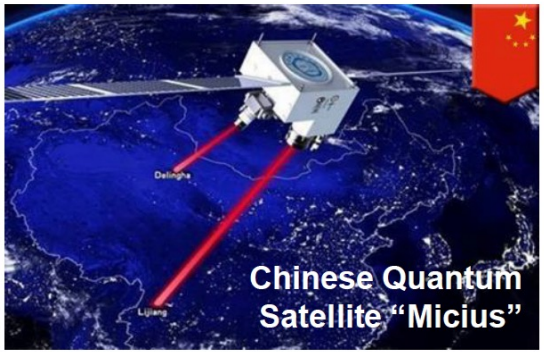
UNIVERSITÄT DES SAARLANDES

Quantensensoren

Atomuhr

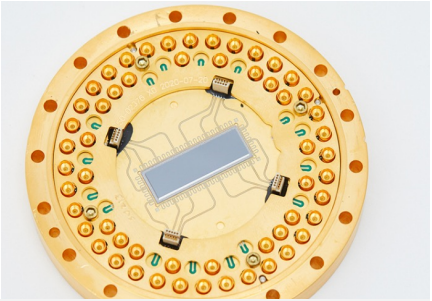
Verbesserte Sensitivität, Auflösung, Genauigkeit

Quantennetzwerke



Sichere Kommunikation, Verteilung von Quanten-zuständen, Quanteninternet

Quantencomputer



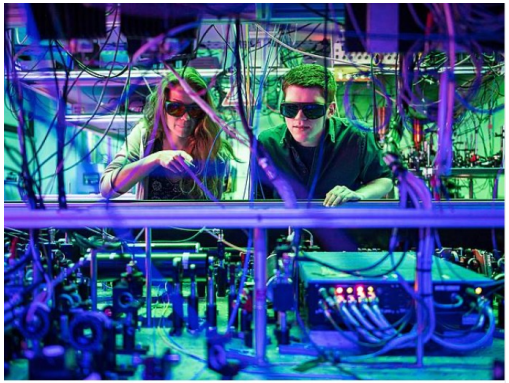
Quantum Processing Unit (QPU) von Rigetti Computing

Beschleunigt bestimmte ausgewählte Rechenprobleme gegenüber klassischen Computern

Quanteninformationstechnologien an der UdS

UNIVERSITÄT DES SAARLANDES

Quantensensoren



© Oliver Dietze

Im Quantenlabor der Universität des Saarlandes

zB. NV, SnV-Zentren in Diamant (Becher)

Quantennetzwerke

Demonstration of quantum network protocols over a 14-km urban fiber link

Stephan Kucera,[1,2] Christian Haen,[1] Elena Arenskötter,[1] Tobias Bauer,[1] Jonas Meiers,[1] Marlon Schäfer,[1] Ross Boland,[3] Milad Yahyapour,[3] Maurice Lessing,[3] Ronald Holzwarth,[3] Christoph Becher,[1,*] and Jürgen Eschner[1,†]

[1] *Experimentalphysik, Universität des Saarlandes, 66123 Saarbrücken, Germany*
[2] *Luxembourg Institute of Science and Technology (LIST), 41 rue du Brill, L-4422 Belvaux, Luxemburg*
[3] *Menlo Systems GmbH, Bunsenstraße 5, 82152 Planegg, Germany*

(Dated: April 9, 2024)

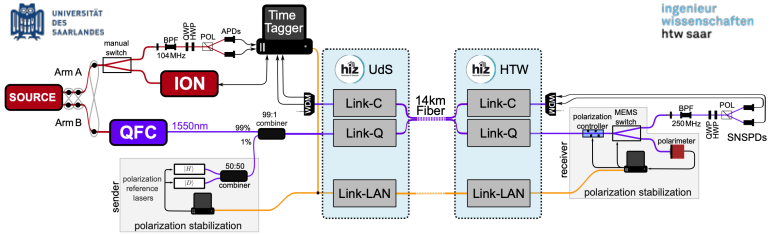


FIG. 8. Overall setup for the quantum communication protocols. Details are provided in the text.

Quantennetzwerk zwischen der UdS und der HTW Saar (Becher, Eschner)

Quantencomputer

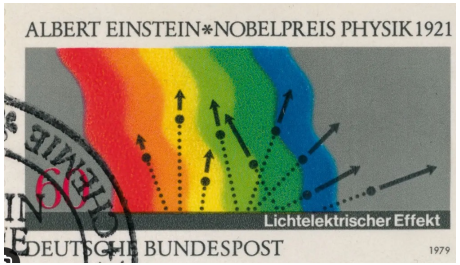
Quantenalgorithmen, Quantenkomplexitätstheorie, Mathematik der Quanteninformation

Mehrere Gruppen in Informatik, Mathematik, und Physik.

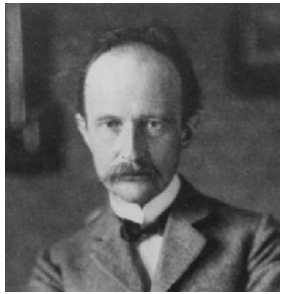
Erste Quantenrevolution: wie alles begann

- Planck (1900): Einführung des Planckschen Wirkungsquantums $\hbar$ zur Erklärung von "schwarzer Strahlung"
- Einstein (1905): Erklärung des lichtelektrischen Effekts durch Einführung von Lichtquanten = Photonen

Einstein (1905)



Es scheint mir nun in der Tat, daß die Beobachtungen über die „schwarze Strahlung", Photolumineszenz, die Erzeugung von Kathodenstrahlen durch ultraviolettes Licht und andere die Erzeugung bez. Verwandlung des Lichtes betreffende Erscheinungsgruppen besser verständlich erscheinen unter der Annahme, daß die Energie des Lichtes diskontinuierlich im Raume verteilt sei. Nach der hier ins Auge zu fassenden Annahme ist bei Ausbreitung eines von einem Punkte ausgehenden Lichtstrahles die Energie nicht kontinuierlich auf größer und größer werdende Räume verteilt, sondern es besteht dieselbe aus einer endlichen Zahl von in Raumpunkten lokalisierten Energiequanten, welche sich bewegen, ohne sich zu teilen und nur als Ganze absorbiert und erzeugt werden können.



Planck (ca. 1900)

Energie eines Photons

$$E = \hbar\omega$$

Impuls eines Photons

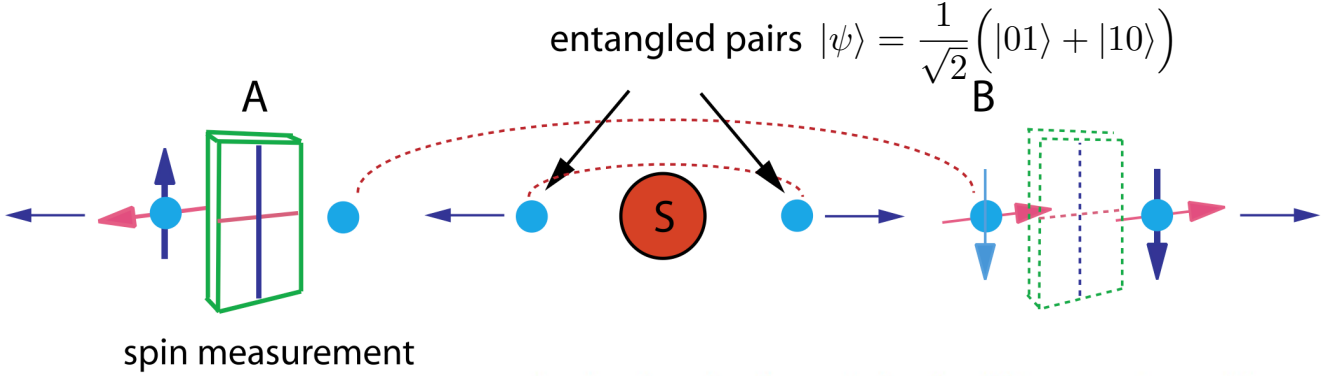
$$p = h/\lambda$$

Drehimpuls eines Photons

$$S = \pm\hbar$$

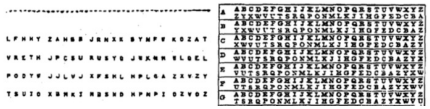
2. Quantenrevolution: von der Theorie zur Anwendung

- Nobelpreis 2022 für A. Aspect, J. F. Clauser, A. Zeilinger für "Experimente mit verschränkten Photonen, die Bell-Ungleichungen verletzen und das Gebiet der Quanteninformation initiiert zu haben".



Anybody who is not shocked by quantum theory has not understood it.
– Niels Bohr

Verschränkung: Währung der Quanteninformation



Einmalverschlüsselungsbuch kann entdeckt werden

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert

Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom

(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

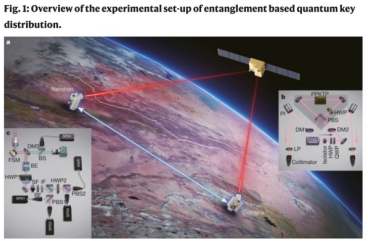
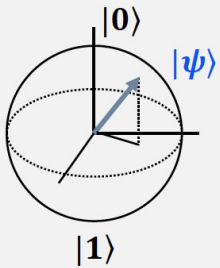


Fig. 1: Overview of the experimental set-up of entanglement based quantum key distribution.

From: J. Lin et al., Nature (2020).

- Sicherer Austausch von privaten Schlüsseln (Einmalverschlüsselung)
- Sicherheit garantiert durch die Gesetze der Physik
- Lauschangriff kann detektiert werden, weil Messung einen Quantenzustand verändert
- Realisiert von Zeilinger et al. in 2007: Verteilung von Schlüsseln zwischen La Palma und Teneriffa & Pan et al. in 2020 via Micius Satellit über 1100 Kilometer

Quantencomputer: tausche Bit für Qubit

	Classical Computer	Quantum Computer
Fundamental logic element	**"Bit" : classical bit** (transistor, spin in magnetic memory, …)	**"Qubit" : quantum bit** (any coherent two-level system)
State	**0 "Or" 1**	 **Superposition:** $\alpha\|0\rangle + \beta\|1\rangle$ $|0\rangle$ **"And"** $|1\rangle$ $\|\psi\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix}$
Measurement	• ***Discrete*** **states** • **Deterministic measurement:** Ex: Set as 1, measure as 1	• ***Superposition*** **states** • **Probabilistic measurement:** Ex: If $\|\alpha\| = \|\beta\|$, 50% $|0\rangle$, 50% $|1\rangle$

© Will Oliver (MIT)

Ein Quantencomputer ist ein programmierbarer Computer, der nach den Gesetzen der Quantenmechanik funktioniert. Die Art wie er Information kodiert ist fundamental verschieden von klassischen Computern.

Quantencomputer: tausche Bit für Qubit

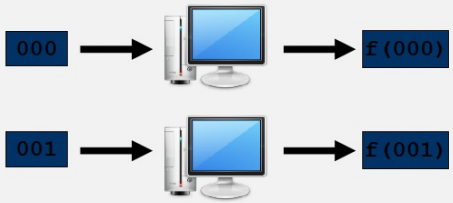
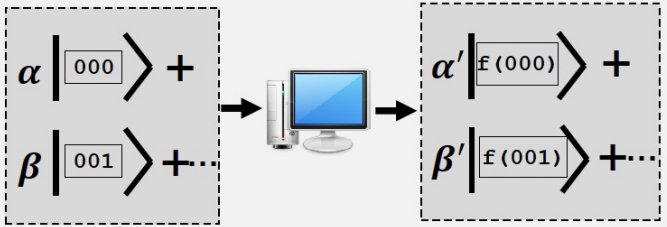
	Classical Computer	Quantum Computer
Fundamental logic element	"Bit" : classical bit (transistor, spin in magnetic memory, …)	"Qubit" : quantum bi… (any coherent two…
State	0 "Or…	$= \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
	…ment: …, measure as 1	• *Superposition* states • Probabilistic measurement: Ex: If $\lvert\alpha\rvert = \lvert\beta\rvert$, 50% $\lvert 0\rangle$, 50% $\lvert 1\rangle$

Mythos 1: "Ein Qubit ist gleichzeitig im Zustand 0 und 1."
Tatsächlich: "Ein Qubit wird durch zwei komplexe Zahlen α und β dargestellt!"

© Will Oliver (MIT)

Ein Q…mputer ist ein programmierbarer Computer, der nach den Gesetzen der Quantenmechanik funktioniert. Die Art wie er Information kodiert ist fundamental verschieden von klassischen Computern.

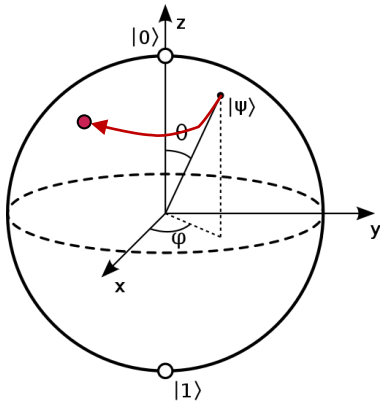
Quantenparallelismus dank Superposition

	Classical Computer	Quantum Computer
Fundamental logic element	**"Bit" : classical bit** (transistor, spin in magnetic memory, …)	**"Qubit" : quantum bit** (any coherent two-level system)
Computing	• N bits: One N-bit state **000, 001, …, 111 (N = 3)** • Change a bit: new calculation (classical parallelism) 	• N qubits: 2^N components to one state $\alpha\|000\rangle + \beta\|001\rangle + \cdots + \gamma\|111\rangle$ (N = 3) • Quantum parallelism & interference 

© Will Oliver (MIT)

Quantengatter: logische Operationen auf Qubits

- Quantengatter verändern den Qubitzustand
- 1-Qubit-Gatter entsprechen Rotationen auf der Blochkugel
- 2-Qubit-Gatter erzeugen Verschränkung zwischen Qubits

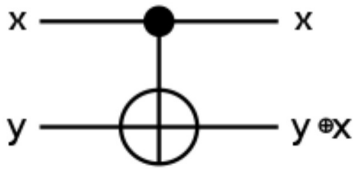


$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

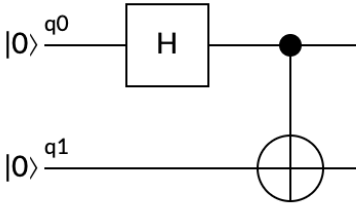
$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Controlled-NOT (CNOT)



$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



$$|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Maximal verschränkter Bell-Zustand

Messungen: was gibt der Quantencomputer aus?

- Messung wandelt Quantenzustand zu klassischer Information
  - Wähle Basis {X, Y, Z} der Messung (Heisenberg'sche Unschärfe)
  - Mögliche Messergebnisse eines Qubits sind Eigenwerte {+1,-1}
  - Messergebnis ist probabilistisch (Born-Regel)

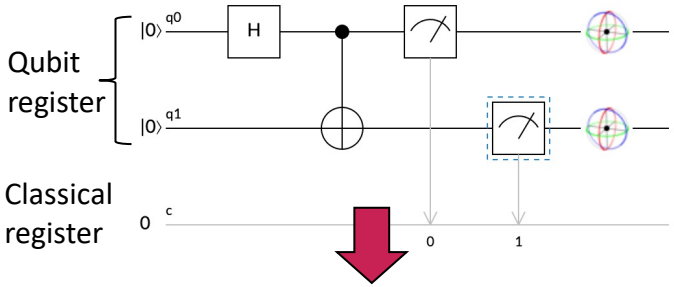
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Messwahrscheinlichkeiten

$$|\langle 00|\psi\rangle|^2 = |\langle 11|\psi\rangle|^2 = 1/2$$

$$|\langle 10|\psi\rangle|^2 = |\langle 01|\psi\rangle|^2 = 0$$

- Quantencomputer gibt am Ende der Rechung einen Bitstring {00101…} zurück
- Wiederholt man die Quantenrechnung, so erhält man viele Bitstrings
- Histogram gegeben durch Wahrscheinlichkeitsverteilung



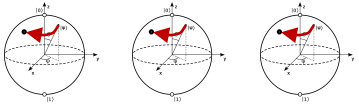
2^10 = 1024: {'11': 501, '00': 523}
2^12 = 4096: {'11': 2035, '00': 2061}
2^14: {'11': 8154, '00': 8230}
2^16: {'11': 32773, '00': 32763}

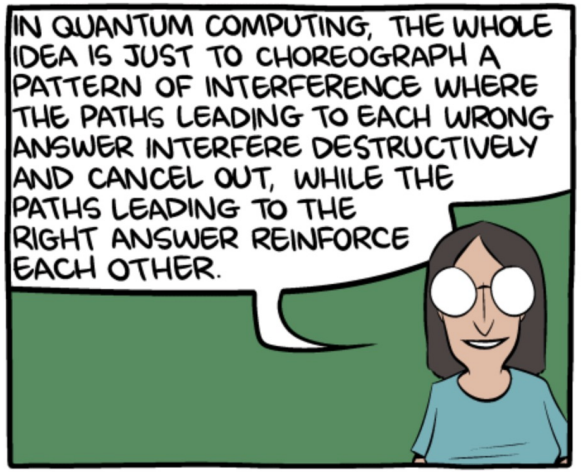
Ergebnisse mehrerer Quanten-rechnungen

Quantencomputer versus klassischer Computer

Figure by C. Addams (NYT)

Wichtigste Unterschiede zwischen Quanten- und klassischen Rechnern

- QC operiert auf Qubitzuständen statt Bits 
- Superposition und komplexe Koeffizienten $c_0 00|000\rangle + c_{001}|001\rangle + \dots$
- Rechenprinzip beruht auf Interferenz verschiedener Rechenpfade, analog zu Wellen- oder Lichtausbreitung
- QC nutzt Verschränkung und daher Nicht-Lokalität der Quantenmechanik
- QC ist intrinsisch probabilistisch (Born-Regel)
- QC kann manche Probleme effizienter lösen als ein klassischer Computer: Zerlegung einer Zahl in Primfaktoren, unstrukturierte Suche, Quantensimulation von physikalischen Systemen



www.scottaaronson.com/blog
smbc-comics.com

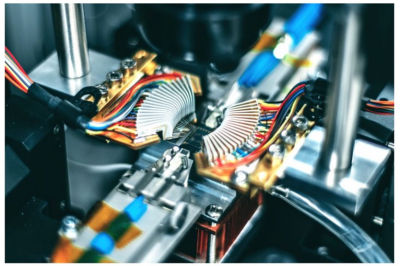
Wie sieht ein heutiger Quantencomputer aus?

UNIVERSITÄT DES SAARLANDES

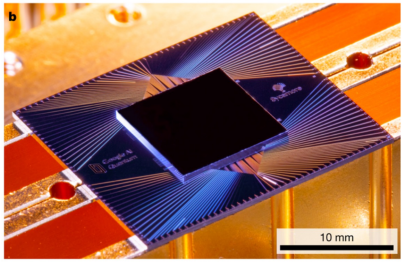
Es gibt verschiedene Hardware-Implementierungen. Zu früh vorrauszusehen, welche sich durchsetzt.

- DiVincenzo Kriterien für skalierbare Quantenrechner
  - Gut charakterisierte Qubits, skalierbar zu großen Systemen
  - Fähigkeit zur Initialisierung & Durchführung von universellen Gattern
  - Lebensdauer des Quantenzustands >> Gatteroperation
  - Fähigkeit zur Messung mit hoher Fidelität
  - Lange Rechnungen sind nur möglich mit Quantenfehlerkorrektur (holy grail)

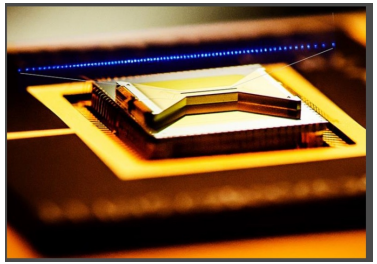
& others (bosonic processors, NVs in diamond,…)



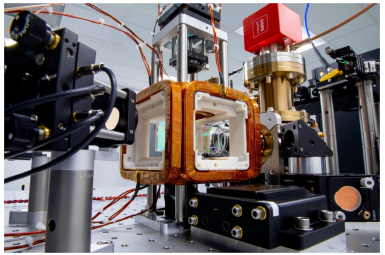
Photonic QC (Xanadu, PsiQ, QuiX, …)



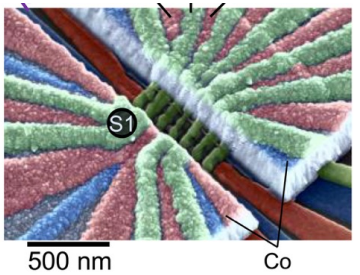
Superconducting qubits (Yale, UCSB, ETH, IBM, Google, Rigetti, Intel…)



Trapped ions (NIST, Innsbruck, IonQ, Quantinuum, Mainz, …)



Neutral (Rydberg) atoms (Harvard, Innsbruck, Paris, QuEra, Pasqal, planQC,..)



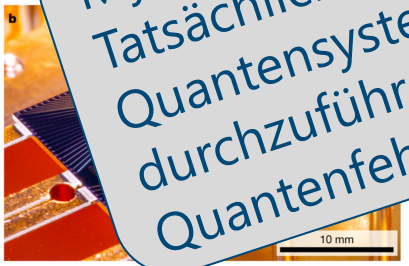
Silicon spin qubits (Princeton, New South Wales, SQC, Intel, …)

Wie sieht ein heutiger Quantencomputer aus?

Es gibt verschiedene Hardware-Implementierungen. Zu früh vorrauszusehen, welche sich durchsetzt.

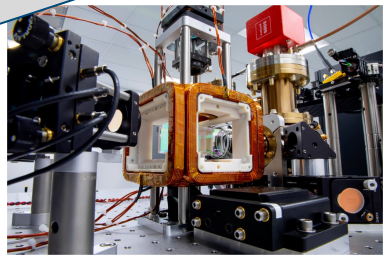
- DiVincenzo Kriterien für skalierbare Quanten, NVs in
  - Gut charakterisierte Qubits, skalierba
  - Fähigkeit zur Initialisierung
  - Lebensdauer des
  - Fähigk
  - (holy grail)

Mythos 2: "Quantencomputing ist unmöglich, zu kompliziert."
Tatsächlich: "Work in Progress: wir haben gelernt kleine Quantensysteme zu kontrollieren und damit Rechnungen durchzuführen. Erste Schritte zur Demonstration von Quantenfehlerkorrektur wurden gezeigt."

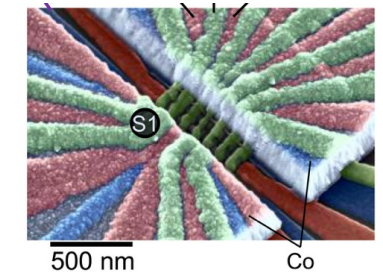


Superconducting qubits (Yale, UCSB, ETH, IBM, Google, Rigetti, Intel…)

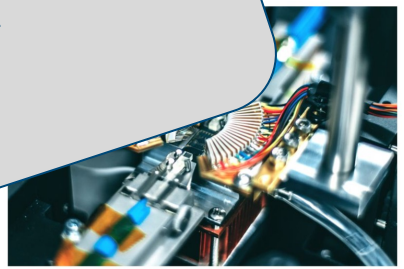
Trapped ions (NIST, Innsbruck, IonQ, Quantinuum, Mainz, …)



Neutral (Rydberg) atoms (Harvard, Innsbruck, Paris, QuEra, Pasqal, planQC,..)



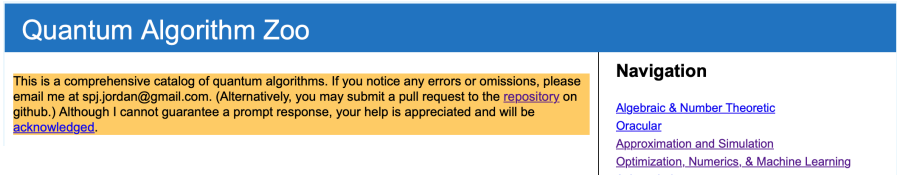
Silicon spin qubits (Princeton, New South Wales, SQC, Intel, …)



Photonic QC (Xanadu, PsiQ, QuiX, …)

Was kann man mit einem Quantencomputer anfangen?

- Work in Progress: derzeit 65 Quantenalgorithmen laut




David Deutsch (Oxford)


Richard Josza (Cambridge)

- Einer der ersten Quantenalgorithmen mit exponentieller Beschleunigung

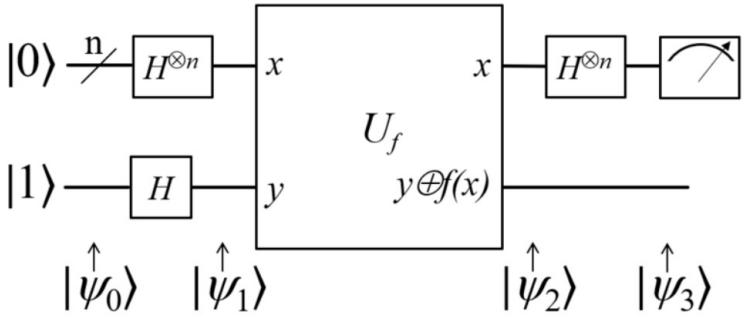
Deutsch's Problem and Deutsch-Josza Algorithmus

Sarah in Saarbrücken sendet eine Zahl $x \in \{0, 2^n - 1\}$ an Bob in Blieskastel. Bob berechnet eine Funktion $f(x) \in \{0,1\}$ and sendet sein Ergebnis. Er verspricht, dass seine Funktion f entweder konstant oder ausgewogen ist, d.h gleich 1 für genau die Hälfte aller Werte x and 0 für die andere Hälfte.

Deutsch-Josza Algorithmus

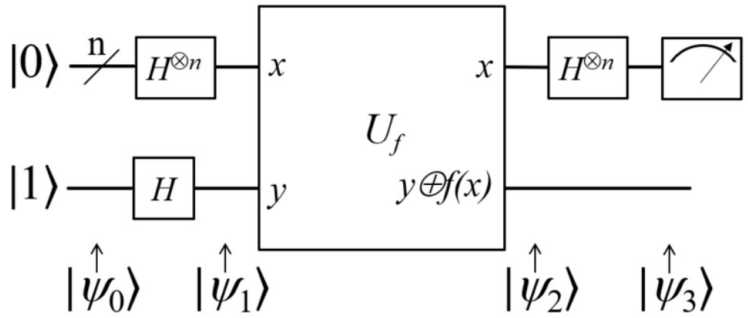
- Im klassischen Fall sendet Sarah einen Wert x nach dem anderen und muss Bob daher im schlimmsten Fall $(2^{n-1}+1)$ Mal fragen, bevor sie weiss ob die Funktion f konstant oder ausgewogen ist.
- Falls Sarah und Bob Qubits austauschen und Bob eine unitäre Transformation verwendet um $f(x)$ zu berechnen, muss Sarah nur 1x fragen!

Exponentielle Beschleunigung



Deutsch-Josza algorithm

Quantenschaltkreis



$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\big(|0\rangle - |1\rangle\big) & \text{if } f(0) = f(1) \\ \pm|1\rangle\big(|0\rangle - |1\rangle\big) & \text{if } f(0) \neq f(1) \end{cases}$$

Beispiel für $n = 1$:

$$|\psi_0\rangle = |01\rangle \longrightarrow |\psi_1\rangle = \frac{1}{2}\Big[|0\rangle + |1\rangle\Big]\Big[|0\rangle - |1\rangle\Big]$$

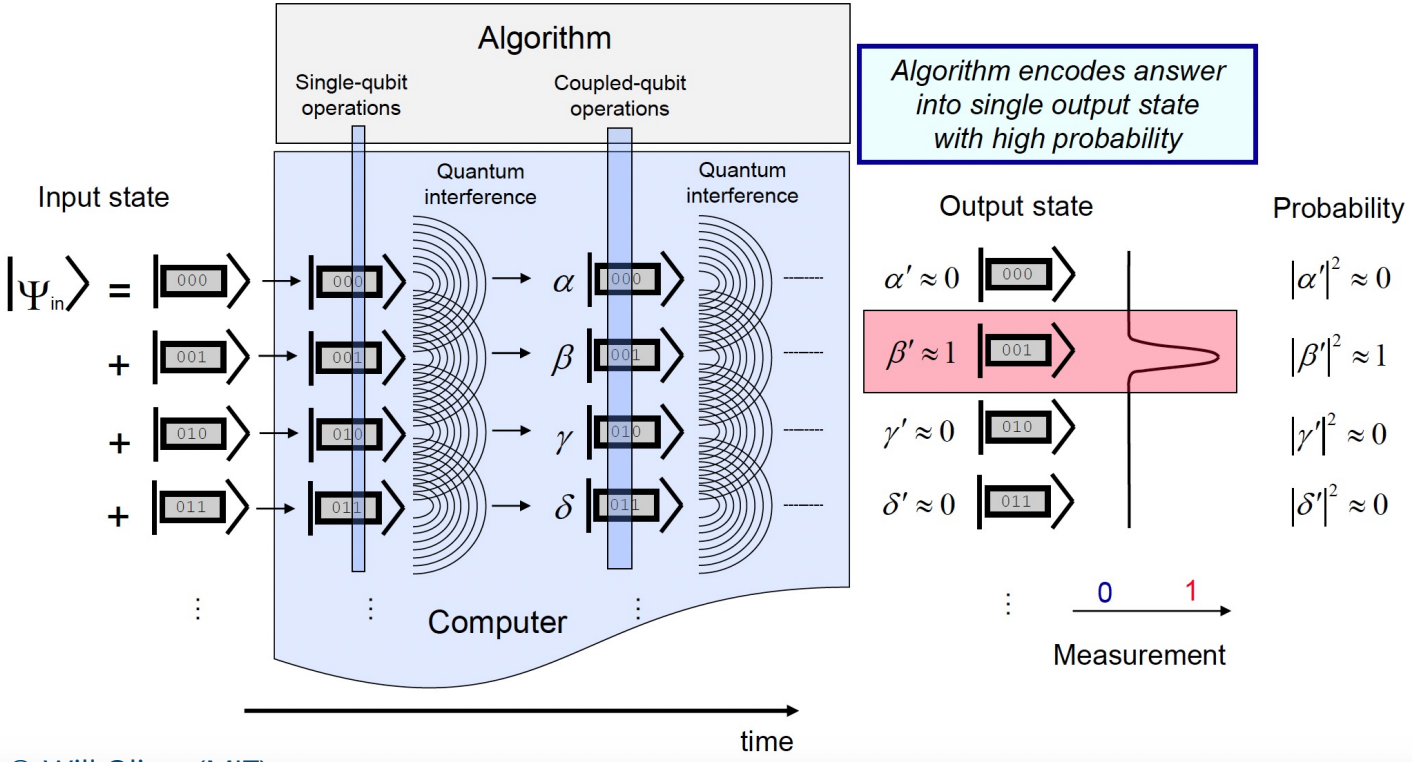
$$|\psi_2\rangle = \frac{1}{2}\Big((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) =$$

$$= \begin{cases} \pm\frac{1}{2}\Big(|0\rangle + |1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) & \text{if } f(0) = f(1) \\ \pm\frac{1}{2}\Big(|0\rangle - |1\rangle\Big)\Big(|0\rangle - |1\rangle\Big) & \text{if } f(0) \neq f(1) \end{cases}$$

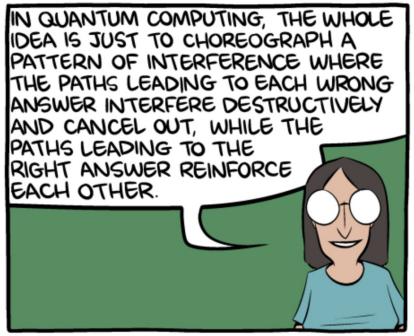
Falls Sarah den Bitstring $|0\rangle^n$ misst, so ist die Funktion konstant. Sonst ist sie ausgewogen.

Verwende: $U_f|x\rangle(|0\rangle - |1\rangle) = (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$

Interferenz zur gewünschten Lösung

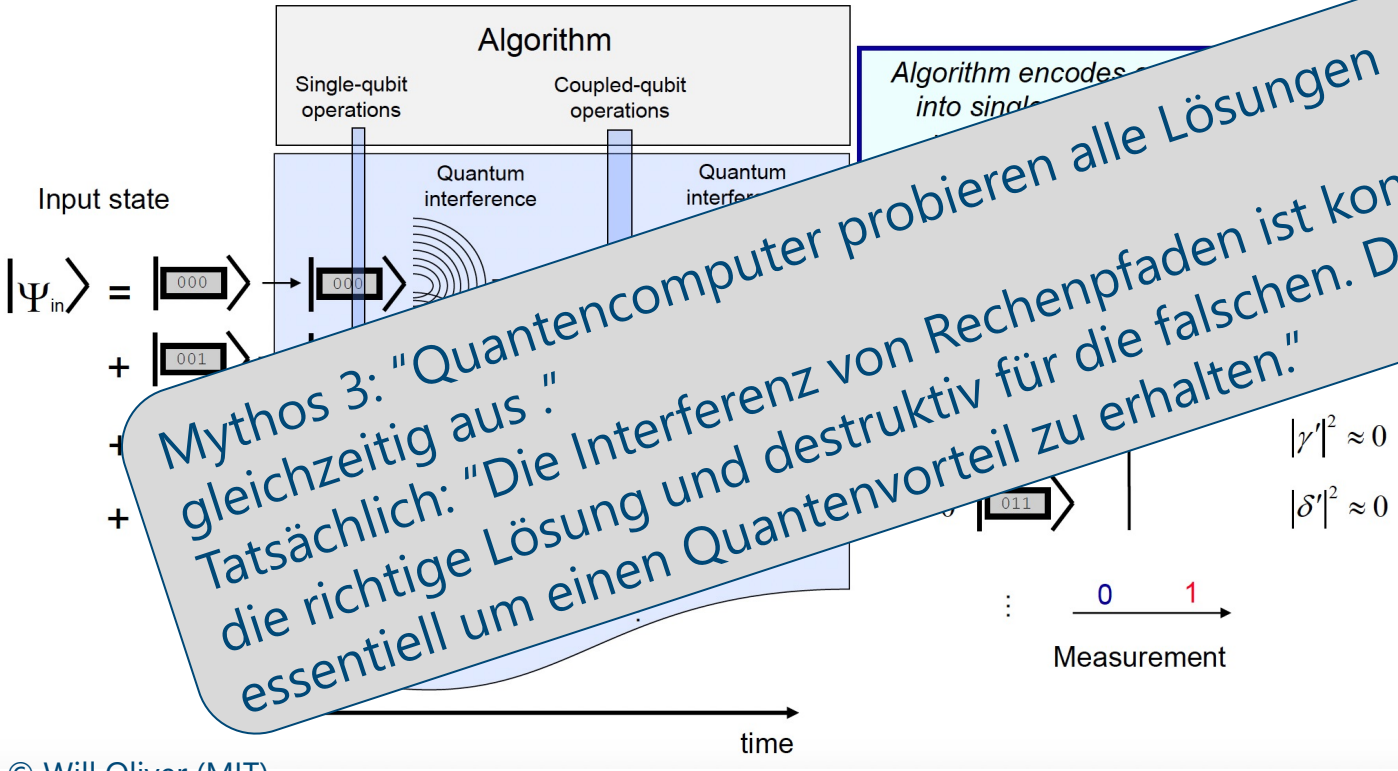


© Will Oliver (MIT)

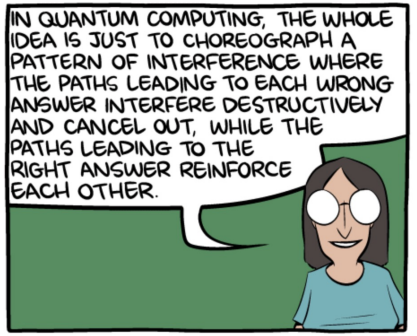


www.scottaaronson.com/blog
smbc-comics.com

Interferenz zur gewünschten Lösung



Mythos 3: "Quantencomputer probieren alle Lösungen gleichzeitig aus."
Tatsächlich: "Die Interferenz von Rechenpfaden ist konstruktiv für die richtige Lösung und destruktiv für die falschen. Das ist essentiell um einen Quantenvorteil zu erhalten."



www.scottaaronson.com/blog
smbc-comics.com

© Will Oliver (MIT)

Was kann man noch mit einem Quantencomputer anfangen?

- Work in Progress
- Viele Anwendungen erfordern Quantenfehlerkorrektur
  - Faktorisierung von Zahlen mit Shor's Algorithmus: knacke RSA Code
    - Beispiel: Knacken eines RSA 2048-bit Schlüssels benötigt ca. 4000 fehlerkorrigierte logische Qubits
    - Knacken der Bitcoin Verschlüsselung benötigt ca. 2300 logische Qubits
  - Quadratische Beschleunigung von unstrukturierter Suche mit Grover's Algorithmus
    - Beispiel: habe Nummer, suche Name dazu im Telefonbuch Saarbrücken mit 180'000 Einträgen: nur 428 Anfragen statt 90'000 sind nötig)
  - Simulation von großen Quantensystemen: Proteinfaltung, Design von Medikamenten, Katalysatoren, Materialien

Codeknacken geht deutlich schneller hiermit…

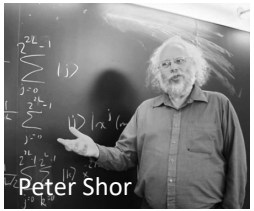
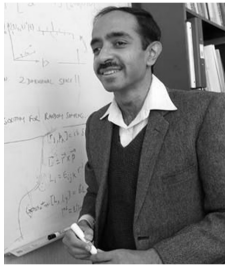
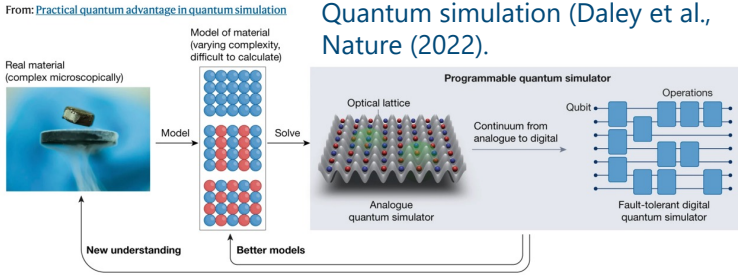


Abbildung 6.1: Unstrukturierte Suche: die Nadel im Heuhaufen

Und Suchen auch …

Lev Grover





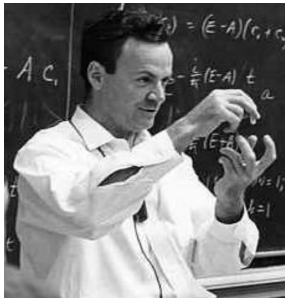
Quantum simulation (Daley et al., Nature (2022).

Simulation von komplexen Quantensystemen

- R. Feynman: “Nature isn't classical, and if you want to make a simulation of Nature, you'd better make it quantum mechanical.”
- Anzahl der Qubitzustände N wächst exponentiell an mit der Anzahl der Qubits: $N = 2^n$
- Beispiel: n=300 → $N = 10^{130} \gg$ Anzahl der Baryonen im Universum $= 10^{80}$
- Kann nicht alle komplexen Zustandsamplituden speichern, aber ein QC erzeugt sie!

Idee: Erzeuge Qubit-Zustand auf dem Computer und messe seine Eigenschaften

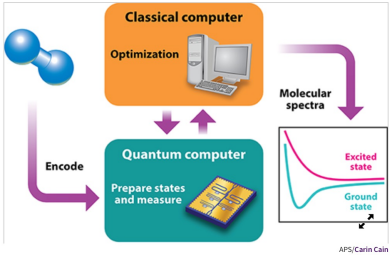
- Bestimme den Grundzustand eines physikalischen Systems und seine Energie
- Simuliere die Quantendynamik die die Zeitentwicklung des Systems beschreibt



Richard Feynman

Was kann man mit einem Quantencomputer anfangen?

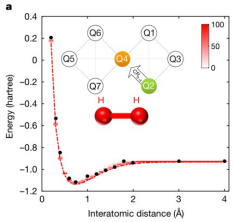
- Work in Progress
- Viele Anwendungen erfordern Quantenfehlerkorrektur
  - Faktorisierung von Zahlen mit Shor's Algorithmus: knacke RSA Code
  - Quadratische Beschleunigung von unstrukturierter Suche mit Grover's Algorithmus
  - Quantensimulation von großen Systemen
- Anwendungen von fehlerhaften, heutigen Quantenrechnern (oftmals heuristisch)
  - Simulation von Quantensystemen, z.B. Bestimmung physikalischer oder chemisch interessanter Wellenfunktionen
  - Simulation von Quantendynamik: chemische Reaktionen, molekulare oder elektronische Dynamik, Proteinfaltung
  - Optimierungsprobleme (z. B. Traveling Salesman), Quanten-KI



Sim, Alán Aspuru-Guzik et al., Physics Viewpoint (2018).

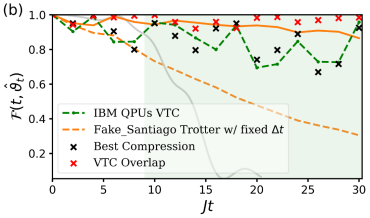
- Klassische Optimierung einer Kostenfunktion, die auf dem Quantencomputer berechnet wird.
- Sehr allgemeines Prinzip!

Präparierung des Grundzustands



Kandala et al (IBM) (2017)

Quantendynamik



Berthusen, PPO et al. (2022)

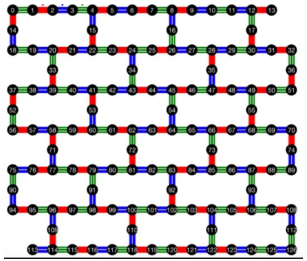
Quantenvorteil: wann ist es soweit?

UNIVERSITÄT DES SAARLANDES

Quantenvorteil: Ein Quantencomputer kann Aufgaben von praktischer Relevanz schneller als jeder verfügbare klassische Supercomputer erledigen.

- Google hatte bereits 2019 einen Quantenvorteil berichtet. “Sycamore” 53 Qubit QPU (Quantum Processing Unit) hat Aufgabe in 200 sec erledigt, die laut den ersten Schätzungn des Google Teams 10’000 Jahre auf klassischer Hardware bräuchte
  - Weiterentwicklung klassischer Algorithmen für dieses speziellen Problem, hat gezeigt, dass man es in wenigen Minuten mit GPUs berechnen kann
  - Take-away: Google’s Rechnung war dennoch ein wichtiger proof-of-principle Schritt (oft verglichen mit dem ersten Flug der Wright Brüder)
- In 2023 hat IBM “quantum utility” berichtet = Quantencomputer ist besser sich selbst zu simulieren als ein klassischer Computer es kann.

Seconds into the first airplane flight, near Kitty Hawk, North Carolina; December 17, 1903, Photo first published in 1908



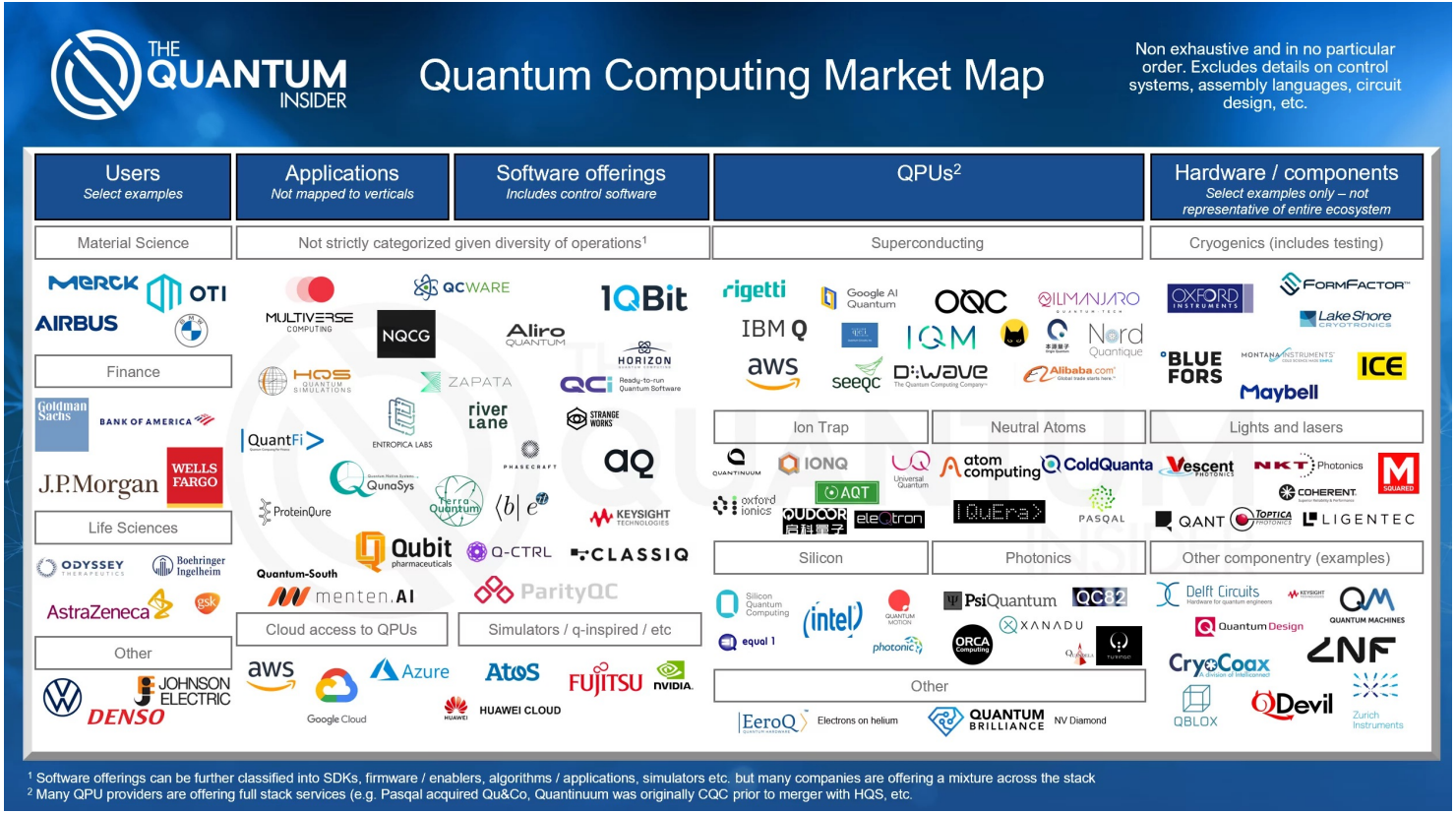
Google Sycamore 53 Qubit QPU

127 qubit IBM QPU

???

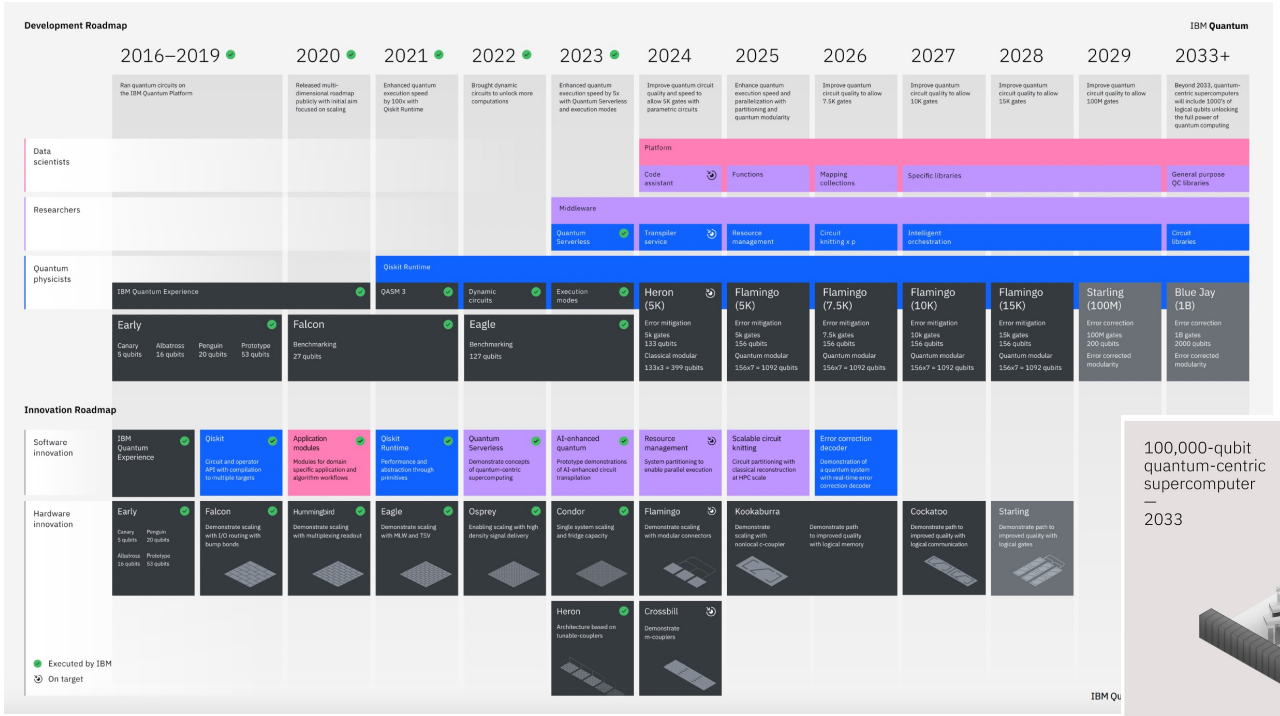
Vermutlich ist Quantenfehlerkorrektur notwendig für einen Quantenvorteil, aber wir wissen es nicht (Forschung!).

Markt der Quantentechnologie: Quantendschungel



Global market summary 2022

Quantencomputer: quo vadis?



Quantenentwicklungs-Roadmap von IBM als Beispiel

Heute: Robledo-Moreno et al., arXiv (2024).

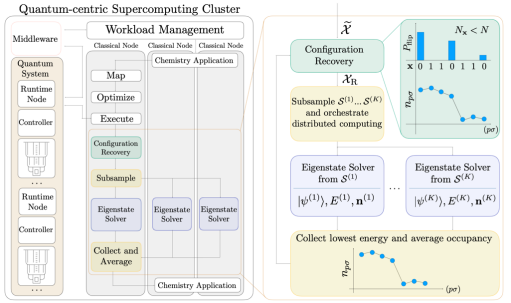
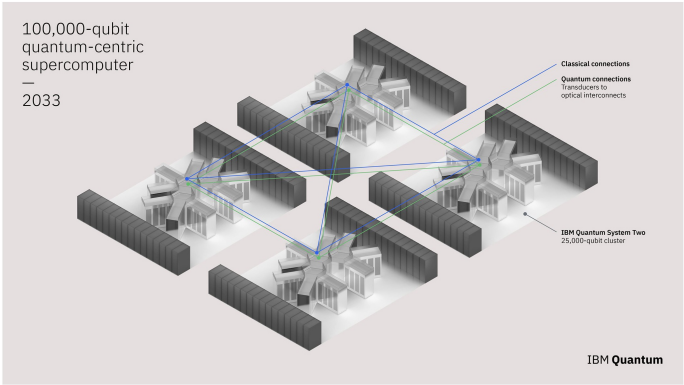


Figure 1. **Quantum-centric supercomputing architecture and workflow diagram. Left:** We illustrate a simplified

In 2033 ???



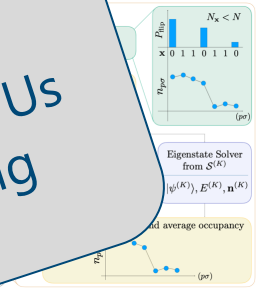
A visual rendering of IBM Quantum's 100,000-qubit quantum-centric supercomputer, expected to be deployed by 2033. (Credit: IBM)

Quantencomputer: quo vadis?

UNIVERSITÄT DES SAARLANDES

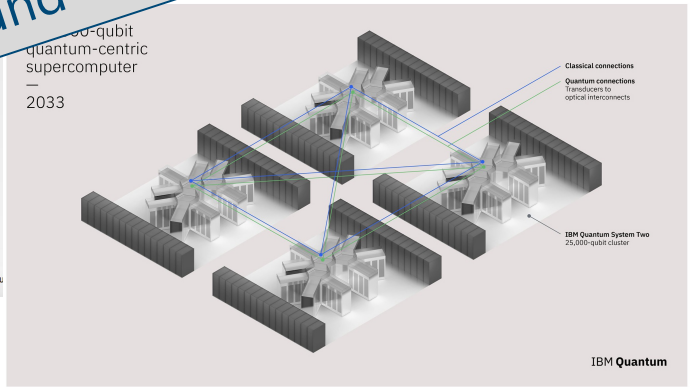
Heute

iv (2024).



puting architecture and workflow diagram. **Left:** We illustrate a simplified

2033 ???



A visual rendering of IBM Quantum's 100,000-qubit quantum-centric supercomputer, expected to be deployed by 2033. (Credit: IBM)

Mythos 4: "Quantencomputer werden digitale klassiche Computer ersetzen."
Tatsächlich: "Quantum Processing Units (QPUs) werden wie GPUs für speziellen Anwendungen eingesetzt, die für CPUs schwierig sind. QPUs sind komplementär zu CPUs und GPUs."

Quantenent ungs-Roadmap von IBM als Beispiel

Zusammenfassung und Ausblick

Thanks for your quantum of attention!

- 2. Quantenrevolution ist im Gange: kontrollierbare Quantensysteme erlauben neue Anwendungen für
  - Quantensensing und Metrologie
  - Quantennetzwerke
  - Quantencomputing

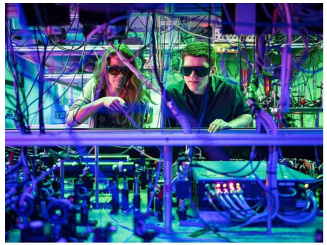
© Oliver Dietze

Im Quantenlabor der Universität des Saarlandes

"You insist that there is something a machine cannot do. If you tell me precisely what it is a machine cannot do, then I can always make a machine which will do just that."

— John von Neumann

- Weitere Forschung und Entwicklung sind notwendig, z.B. um
  - Quantenfehlerkorrektur zu realisieren
  - Neue Quantenalgorithmen zu entwickeln und zu testen
  - Anwendungen mit Quantenvorteil zu finden
- Weitere Worte zu finden, an die man "Quantum" voranstellen kann



© Oliver Dietze

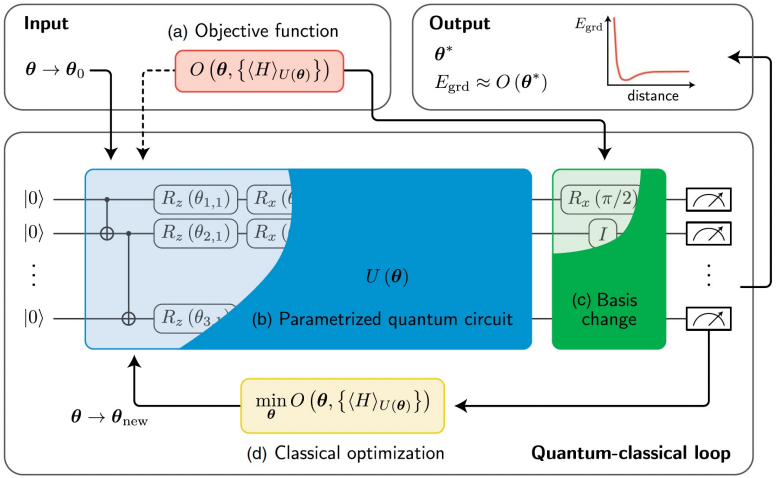
Im Quantenlabor der Universität des Saarlandes

Backup Slides

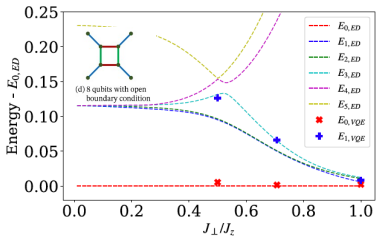
Noisy intermediate-scale quantum computing (NISQ) era

- Without error correction, errors accumulate over time: maximal gate depth is limited
- Near-term applications:
  - Generate truly random numbers by sampling from a random wavefunction
  - Simulate short time dynamics using shallow circuits
  - Simulating ground and excited state properties via hybrid quantum-classical algorithms
  - Solve optimization problems (approximately)

From Bharti et al. (2022).

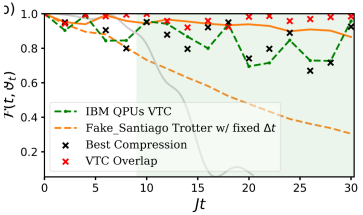


Ground state preparation



Li, PPO et al. (2023).

Quantum dynamics

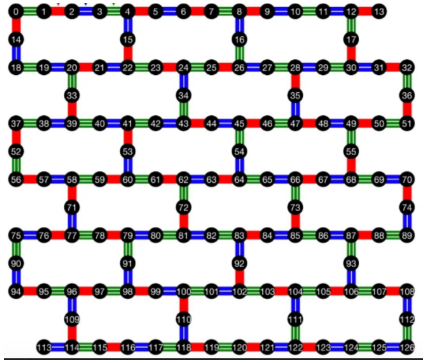


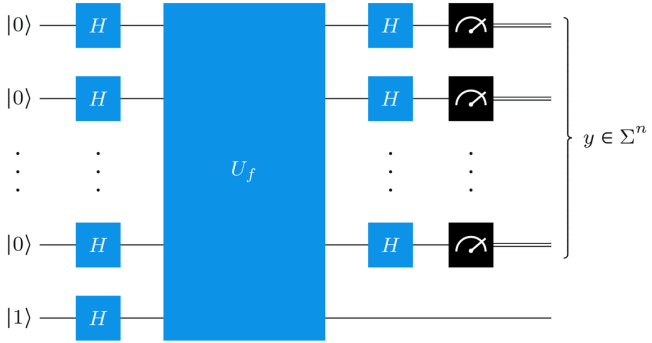
Berthusen, PPO et al. (2022)

Noisy versus fault-tolerant era of quantum computing

- Entangling many qubits is challenging!
- Need to compile it up into natively implementable gates on QPU (quantum processing unit)
- Results in deep circuits. Execution on noisy hardware requires quantum error correction!

127 qubit IBM QPU





Balanced oracle