Quantencomputer: Vision und Wirklichkeit

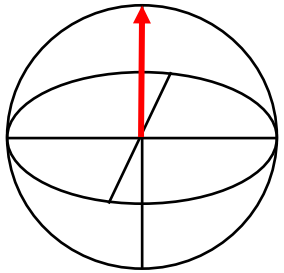
Martin Gärttner

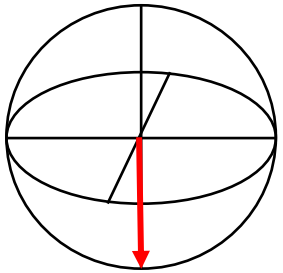
Universität Heidelberg

GI Kolloquium, SRH, 19.10.2021

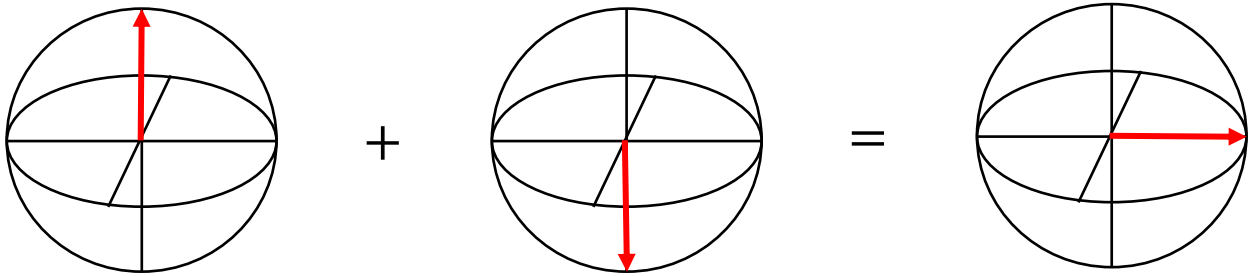
Funding:

Bits vs. Qubits

$0 =$ 

$1 =$ 

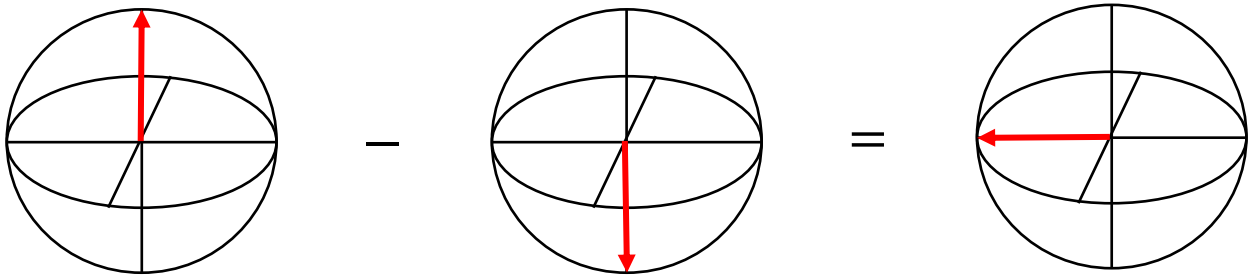
Klassisch: Diskrete Zustände

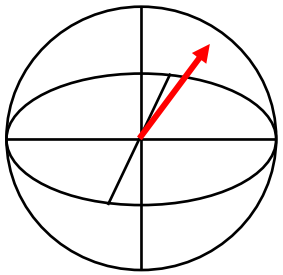


Quantenmechanisch: Superposition

Mathematisch: Zustandsvektor

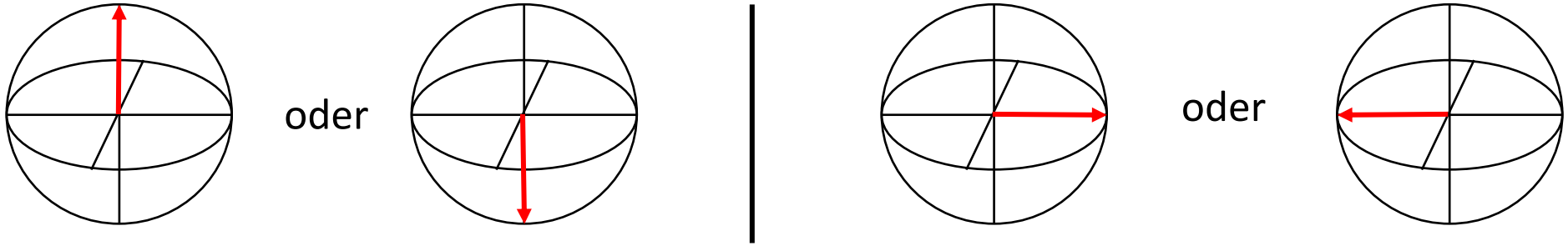
$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle$$





Physikalische Konsequenzen

Es gibt physikalische Eigenschaften, die nichtgleichzeitig festgelegt sein können.



Welches Ergebnis man erhält (0 oder 1) entscheidet sich erst bei der Messung.

Die Messung ändert den Zustand.

Einstein, Podolsky, Rosen (1935): Quantenmechanik kann keine vollständige Beschreibung der Natur sein.

Bell (1964): Bellsche Ungleichungen: Klassische “Vervollständigungen” können ausgeschlossen werden.

Viele bits vs. viele Qubits

Bit Register ist zu jedem Zeitpunkt in **diskretem Zustand**:

2 bits: $|01\rangle$ 3 bits: $|101\rangle$ 4 bits: $|1011\rangle$ usw.

Qubit Register kann in beliebiger **Superposition** sein:

2 Qubits: $c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$

3 Qubits: $c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6|110\rangle + c_7|111\rangle$

Exponentielle Skalierung

Komplexität der Beschreibung von Quantenvielteilchensystemen

Inhärente Parallelität

Idee des quantenmechanischen Computers

Richard Feynman (1982):

Quelle: Wikipedia

“Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.”

"Simulating Physics with Computers". *International Journal of Theoretical Physics*. **21** (6–7): 467–488

Peter Shor (1994):

Quelle: Wikipedia

“Algorithms for quantum computation: discrete logarithms and factoring”

Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134

Der Quantencomputer

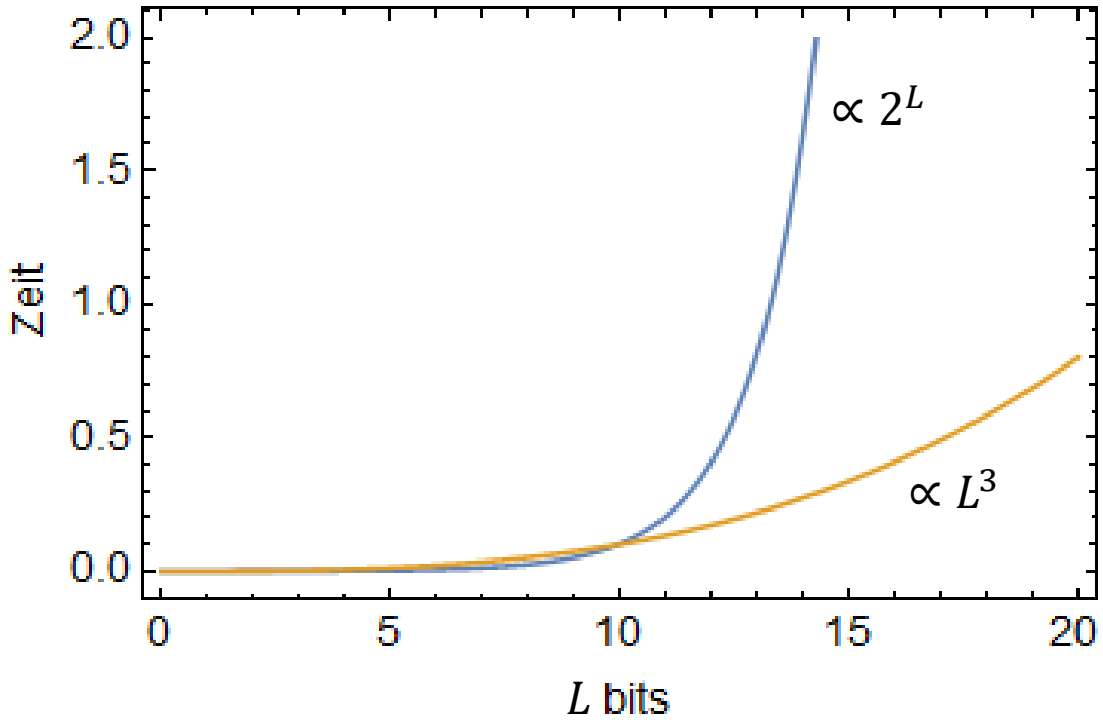
1. Ist er realisierbar?

2. Was können wir damit machen?

- Shor‘s Algorithmus (und andere, verwandte Algorithmen, Grover)

Shor‘s Algorithmus: Primzahlzerlegung

$15 = 3 * 5$	4 bits
$91 = 7 * 13$	7 bits
$9301 = 71 * 131$	14 bits
$N = p * q$	L bits



Relevanz für Kryptographie
RSA Verfahren

Reduktion auf Order Finding

Ziel: Finde b, sodass

$$b^2 = 1 \bmod N$$

$$b^2 = 1 + mN$$

$$b^2 - 1 = mN$$

$$(b+1)(b-1) = mN$$

$\Rightarrow b+1$ und $b-1$ haben gemeinsamen Teiler mit N
(außer wenn $b = \pm 1 \bmod N$)

Satz von Euler: Für a teilerfremd zu N, gibt es ein (kleinstes) $r < N$, sodass

$$a^r = 1 \bmod N$$

Wenn r gerade und $a^{r/2} \neq -1 \bmod N$, dann ist $a^{r/2}$ das gesuchte b und wir müssen nur noch $\mathrm{ggT}(b \pm 1, N)$ berechnen.

Shor‘s Algorithmus, klassischer Teil

Gegeben N, suche Faktor

1. Wähle a $< N$ zufällig

   Falls $\mathrm{ggT}(a, N) > 1$, Ende

2. Berechne r, sodas $a^r = 1 \bmod N$

   Falls r gerade & $a^{r/2} \neq -1 \bmod N$, Ende

   Andernfalls, gehe zu 1.

Periode von $f(x) = a^x \bmod N$???

Beispiel: $N = 15$

$$a = 7$$

$$7 * 7 = 49 = 4\ mod\ 15$$

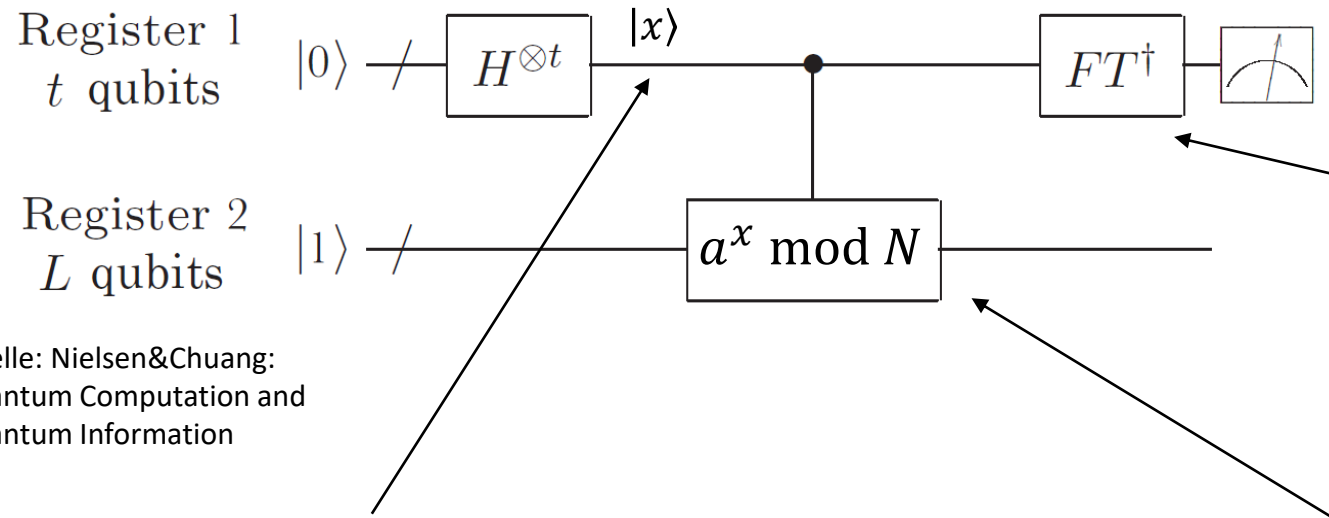
$$4 * 7 = 28 = 13\ mod\ 15$$

$$13 * 7 = 91 = 1\ mod\ 15$$

$$\Rightarrow r = 4 \qquad b = 4$$

$$\Rightarrow (4 + 1)(4 - 1) = m * 15$$

Shor‘s Algorithmus: Quanten-Teil



Quelle: Nielsen&Chuang: Quantum Computation and Quantum Information

Messung

Quanten-Fourier-Transformation: Periode extrahieren

Wende $f(x)$ auf alle x gleichzeitig an!
Quanten-Parallelität!

$$|0 \dots 00\rangle + |0 \dots 01\rangle + |0 \dots 11\rangle + \cdots + |1 \dots 11\rangle$$

Alle Zahlen von 0 bis $2^t - 1$

Skalierung der Anzahl der Qubits: $2^L = N,\ t = 2L$
Anzahl Gatter-Operationen: $L^2 \log L$

RSA: 2048 bit

Der Quantencomputer

1. Ist er realisierbar?

- Physikalische Qubits
- Qubit race

2. Was können wir damit machen?

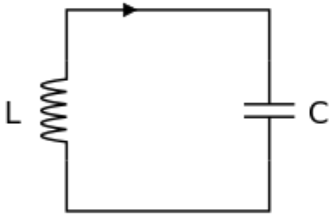
- Shor‘s Algorithmus

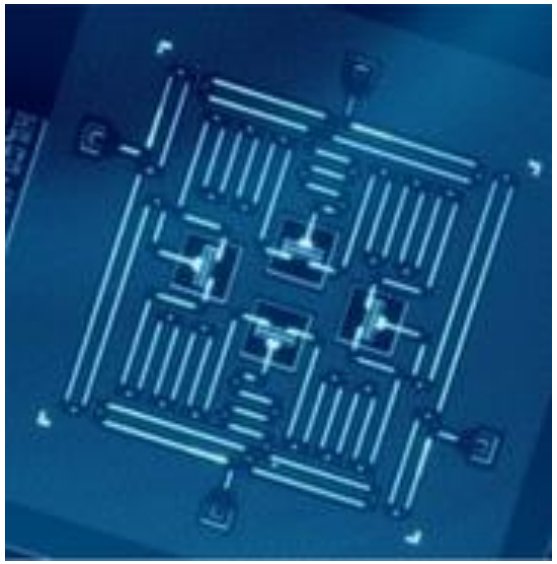
Physikalische Qubits

Supraleitende Qubits

Qubit = Quantisierte Zustände im Schwingkreis

Kontrolle: Mikrowellen



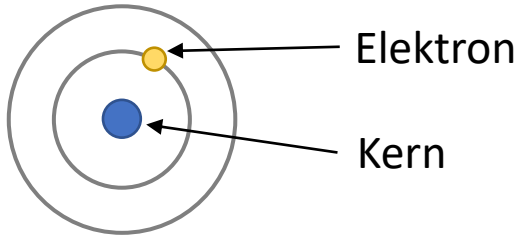


Quelle: Wikipedia

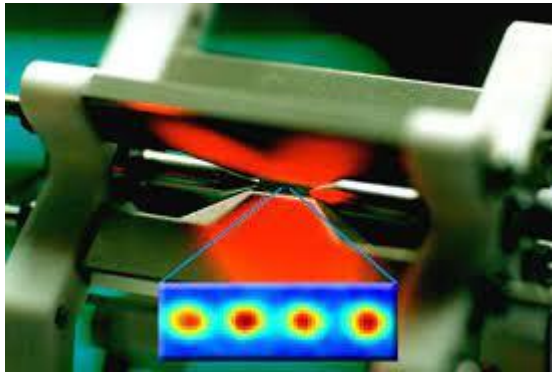
Ionen und kalte Atome

Qubit = Anregungszustände des Valenzelektrons

Kontrolle: Laser



z.B. Ca^+



Photonen, Quantenpunkte, Elektronenspin, Majorana-Moden, Kernspins…

Quantencomputer programmieren

IBMQ: Quiskit

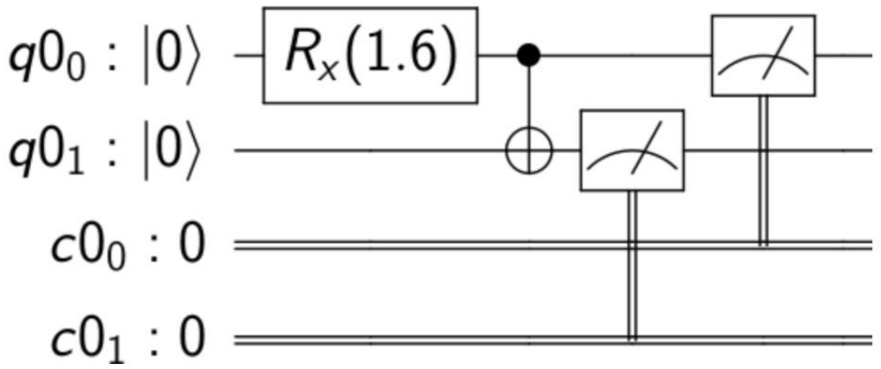
Microsoft: Q#

Google: Cirq

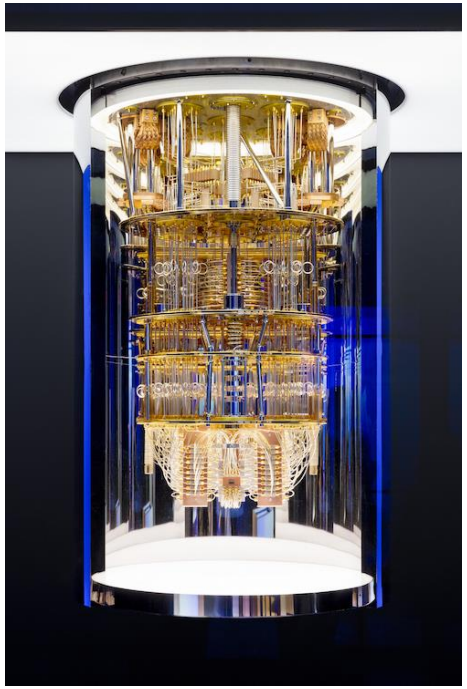
...

In [7]:
```
from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
from qiskit.tools.visualization import circuit_drawer
import numpy as np

qr = QuantumRegister(2)
cr = ClassicalRegister(2)
qp = QuantumCircuit(qr,cr)

qp.rx( np.pi/2,qr[0])
qp.cx(qr[0],qr[1])

qp.measure(qr,cr)

circuit_drawer(qp)
```

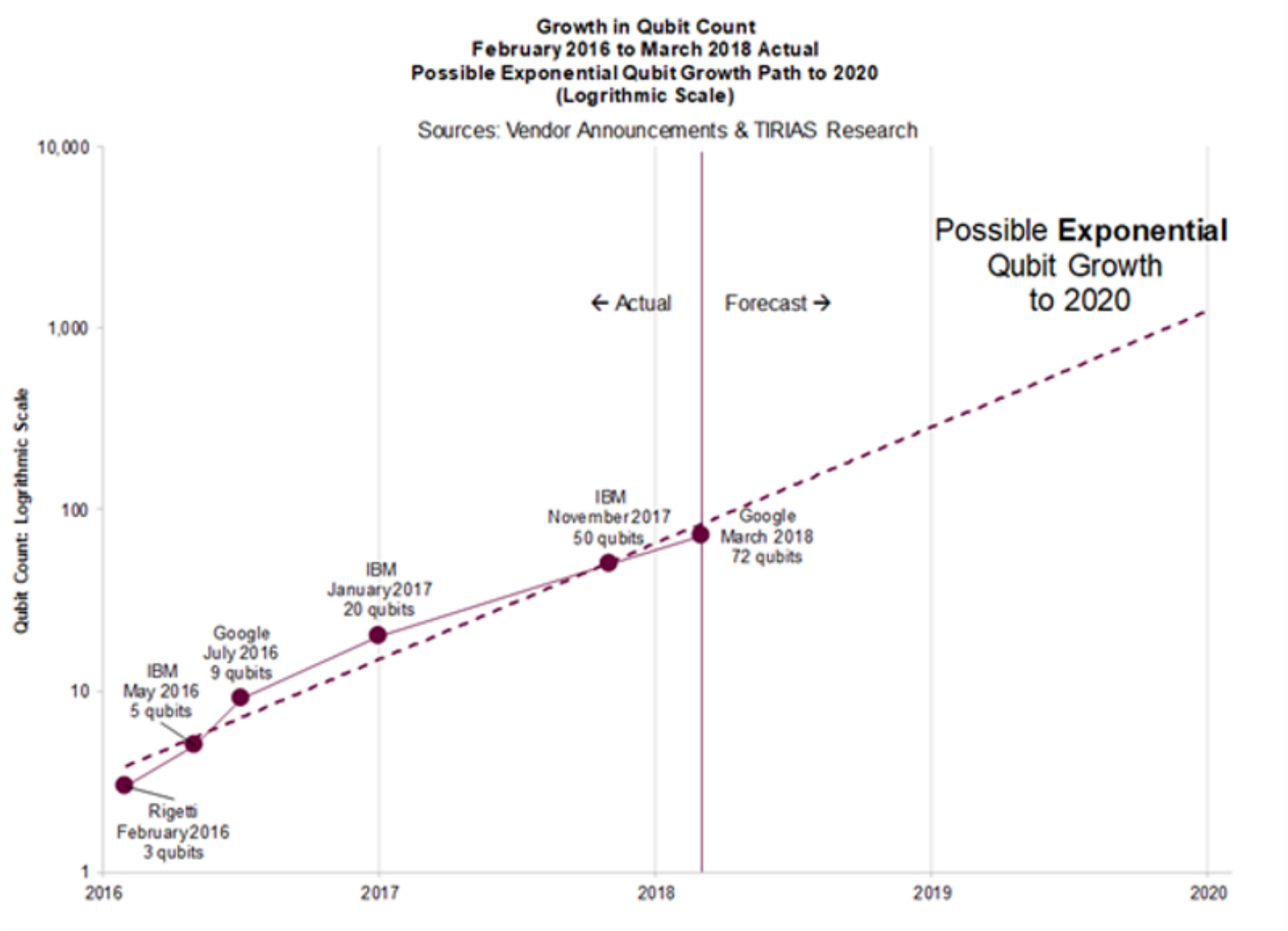
Out[7]:



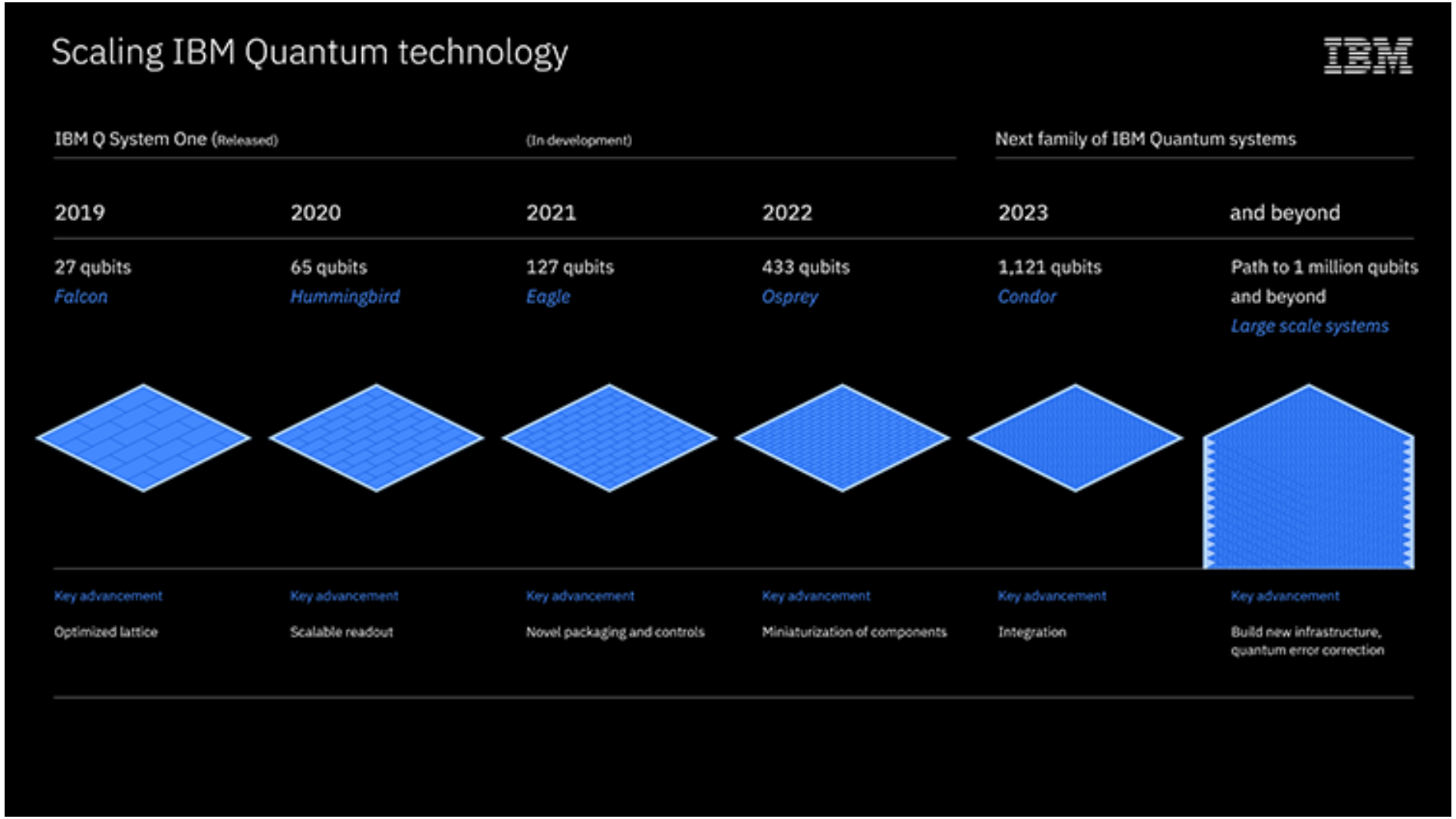
Quelle: IBMQ



Qubit race


Growth in Qubit Count
February 2016 to March 2018 Actual
Possible Exponential Qubit Growth Path to 2020
(Logrithmic Scale)
Sources: Vendor Announcements & TIRIAS Research
Qubit Count: Logrithmic Scale
10,000
1,000
100
10
1
2016
2017
2018
2019
2020
← Actual
Forecast →
Possible Exponential Qubit Growth to 2020
Rigetti February2016 3 qubits
IBM May 2016 5 qubits
Google July 2016 9 qubits
IBM January2017 20 qubits
IBM November2017 50 qubits
Google March 2018 72 qubits

Qubit race


Scaling IBM Quantum technology
IBM
IBM Q System One (Released)
(In development)
Next family of IBM Quantum systems
2019
2020
2021
2022
2023
and beyond
27 qubits
Falcon
65 qubits
Hummingbird
127 qubits
Eagle
433 qubits
Osprey
1,121 qubits
Condor
Path to 1 million qubits and beyond
Large scale systems
Key advancement
Optimized lattice
Key advancement
Scalable readout
Key advancement
Novel packaging and controls
Key advancement
Miniaturization of components
Key advancement
Integration
Key advancement
Build new infrastructure, quantum error correction

Der Quantencomputer

1. Ist er realisierbar?

- Physikalische Qubits
- Qubit race
- Fehler und Fehlerkorrektur
- Threshold theorem

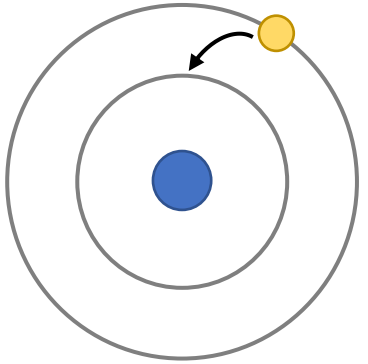
2. Was können wir damit machen?

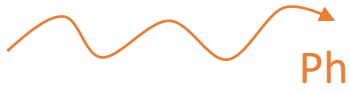
- Shor‘s Algorithmus

Fehleranfälligkeit

Kopplung an Umgebung, Zerfall

→ Überlagerung wird zerstört

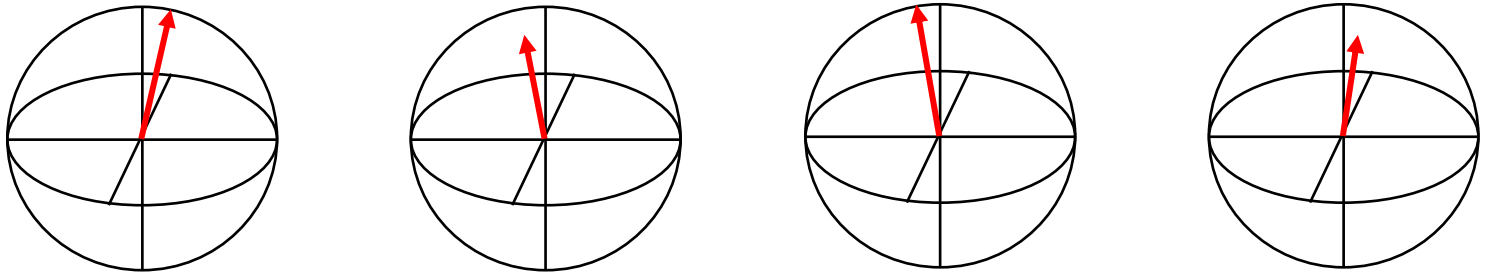




$$|1\rangle \rightarrow |0\rangle$$

$$c_0|0\rangle + c_1|1\rangle \rightarrow |0\rangle$$

Rauschen: Dekohärenz (Problem kontinuierlicher Repräsentation)



Quantenfehlerkorrektur

Klassische Fehlerkorrektur: Redundanz

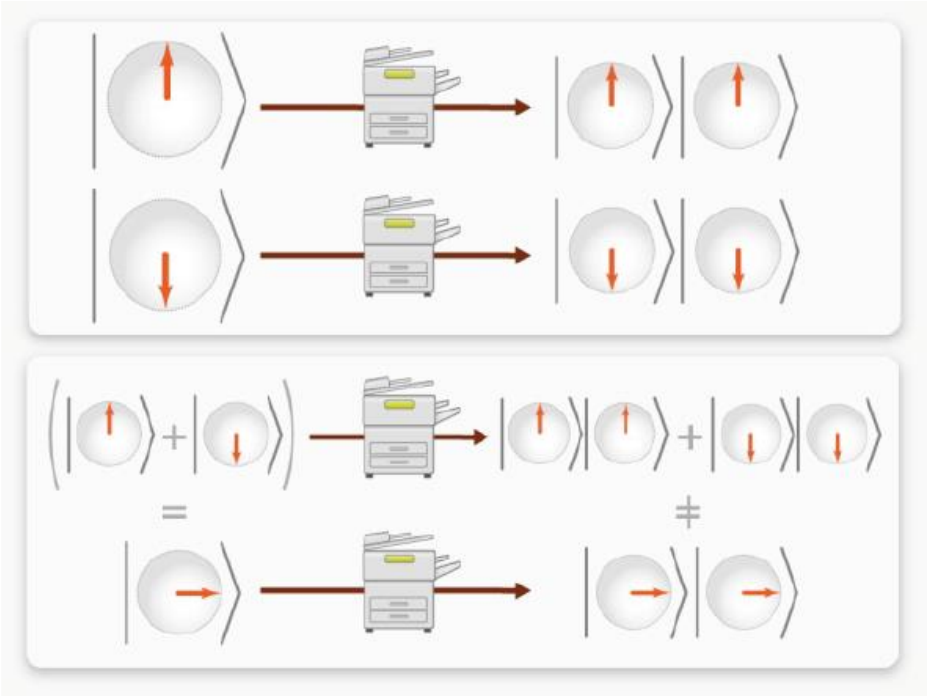
$$|1011\rangle \quad |1011\rangle \quad |1011\rangle$$
$$\downarrow \qquad \downarrow \qquad \downarrow$$
$$|1000\rangle \quad |1000\rangle \quad |1100\rangle$$

Quantenmechanisch:

Kein Kopieren!

Kein naives Messen!

$$c_0|0\rangle + c_1|1\rangle \rightarrow |0\rangle$$



Quelle: W. Dür, S. Heusler, arXiv:1312.1463

Quantenfehlerkorrektur

Quantenmechanische Redundanz

→ Messung der Fehler ohne Zustandsmessung

Logisches qubit	Kodiertes qubit
$\|0\rangle$	$\|000\rangle$
$\|1\rangle$	$\|111\rangle$

Messung:

Vergleich von Qubits!!

	Q1=Q2?	Q2=Q3?
Kein Fehler		
Fehler Q1		
Fehler Q2		
Fehler Q3		

Enkodierung Fehler

$$c_0|0\rangle + c_1|1\rangle \quad \rightarrow \quad c_0|000\rangle + c_1|111\rangle \quad \rightarrow \quad c_0|100\rangle + c_1|011\rangle$$

Threshold theorem

Brauche viele qubits!

Der Quantencomputer

1. Ist er realisierbar?

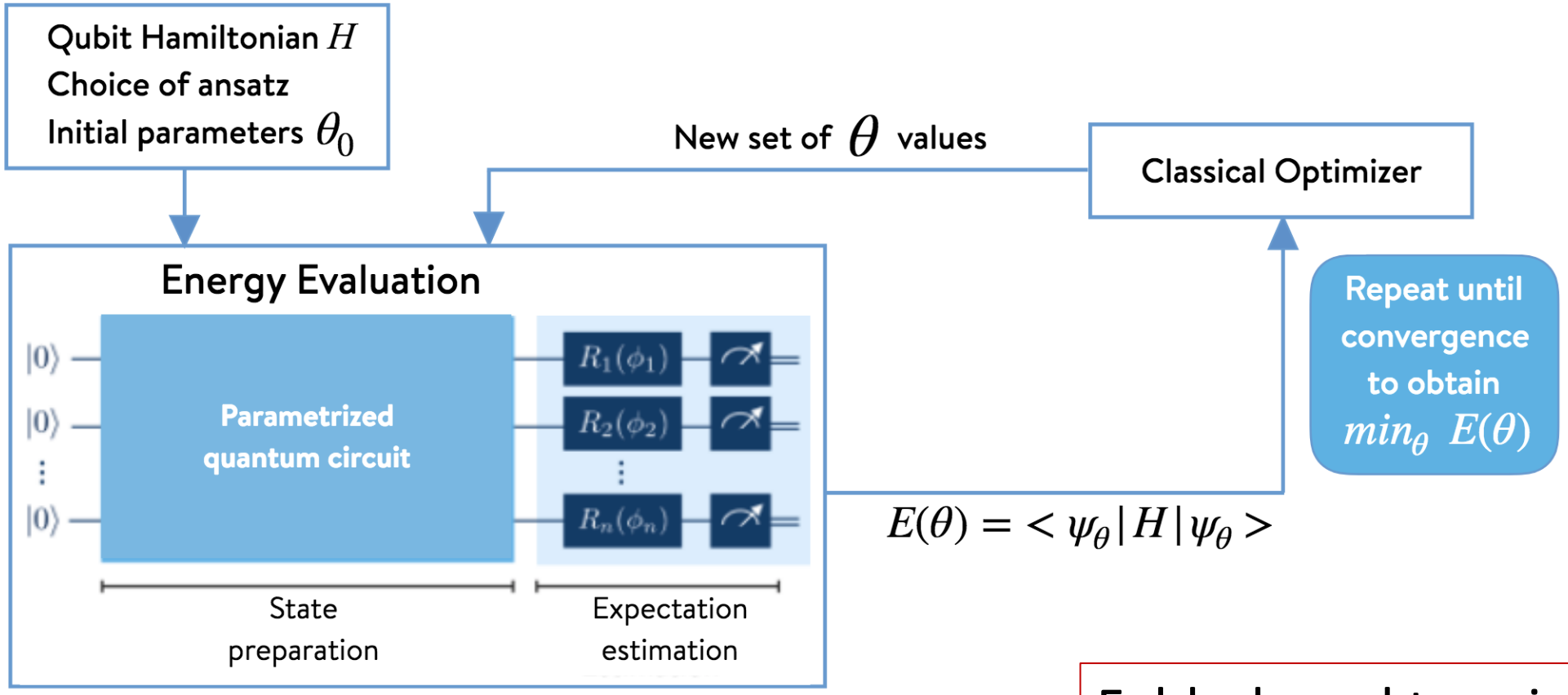
- Physikalische Qubits
- Qubit race
- Fehler und Fehlerkorrektur
- Threshold theorem

2. Was können wir damit machen?

- Shor‘s Algorithmus
- Quanten-Klassische Hybrid Algorithmen
- Quantensimulation

Hybridalgorithmen: Variational Quantum Eigensolver (VQE)

Quantenchemie: Molekül mit vielen Elektronen → Grundzustand?



Quelle: 1QBit

Fehlerkorrektur nicht nötig!

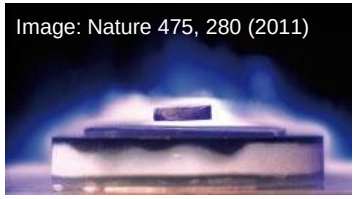
(Analoge) Quanten-Simulation

Quantenmechanische Systeme schwer zu simulieren (klassisch)

Feynman: Simulating physics with computers (1982)

And I'm not happy with all the analyses that go with just the classical theory, because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.

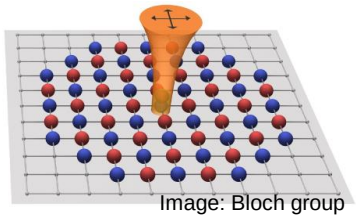
Special purpose Quantencomputer



beschreibt

$\hat{\mathcal{H}}$

emuliert



Physikalisches System | Mathematisches Modell | Quanten-Simulator

Hochtemperatur-Supraleitung, Festkörperphysik,…

Quantencomputer: Vision und Wirklichkeit

Quantum supremacy in der Theorie

Anwendungen innerhalb der Physik

Echte Skalierbarkeit? Killer App?

„Fuss-in-der-Tür“ Investitionen

Keine falschen Versprechungen

Spannende Zeiten für Quantenphysiker!

Danke für Ihre Aufmerksamkeit!

Danke an Michael Marthaler, von dem ich mir einige Ideen geliehen habe.

Backup Folien

Quantum Machine Learning

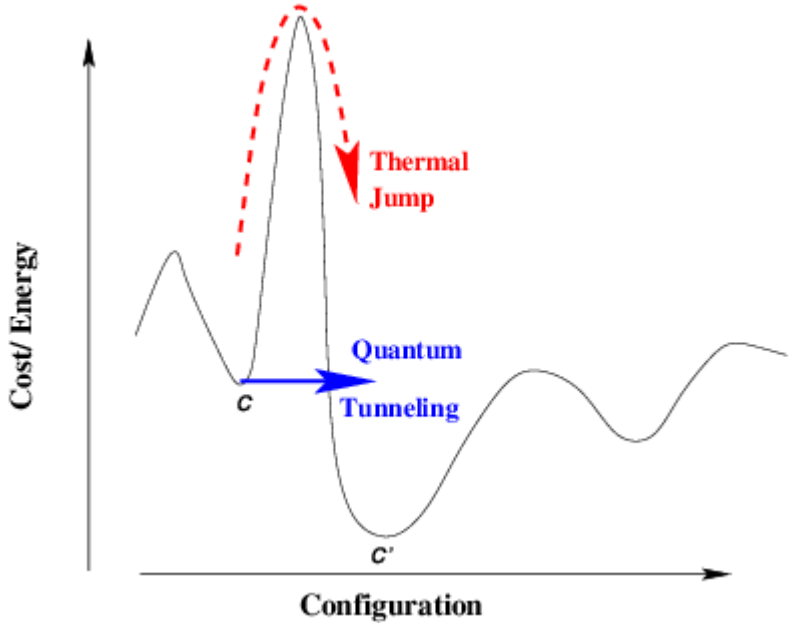
Really?

Quelle: The Quantum Daily

Quantum annealing

No quantum advantage demonstrated yet

Quelle: The Quantum Daily



Quelle: Wikipedia

Quantum supremacy paper (and reactions)

Article

Quantum supremacy using a programmable superconducting processor

Nature 574, 505–510 (2019)

Zufalls-Schaltkreise

Bis 53 Qubits

Fidelity ~0.002

Klassische Simulierbarkeit?

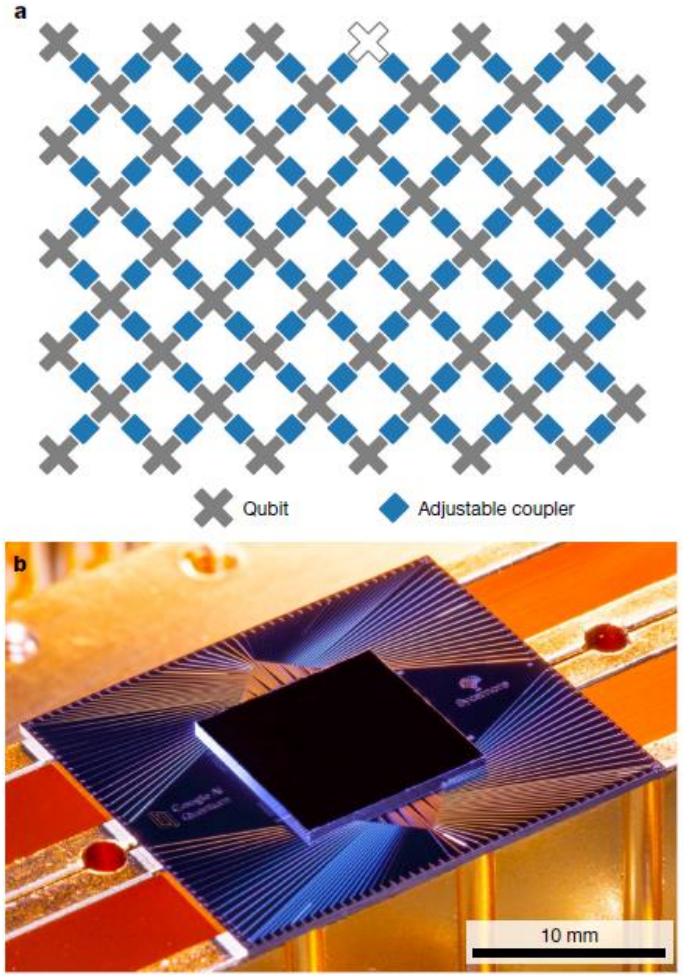


Fig. 1 | The Sycamore processor. a, Layout of processor, showing a rectangular array of 54 qubits (grey), each connected to its four nearest neighbours with couplers (blue). The inoperable qubit is outlined. **b**, Photograph of the Sycamore chip.