UNIVERSITÄT PADERBORN
Die Universität der Informationsgesellschaft

Introduction to Quantum Computing

Dr. Robert Schade
HPC-Advisor
Paderborn Center for Parallel Computing
Paderborn University

Paderborn Center for Parallel Computing

September 2020

Introduction to Quantum Computing

Paderborn Center for Parallel Computing

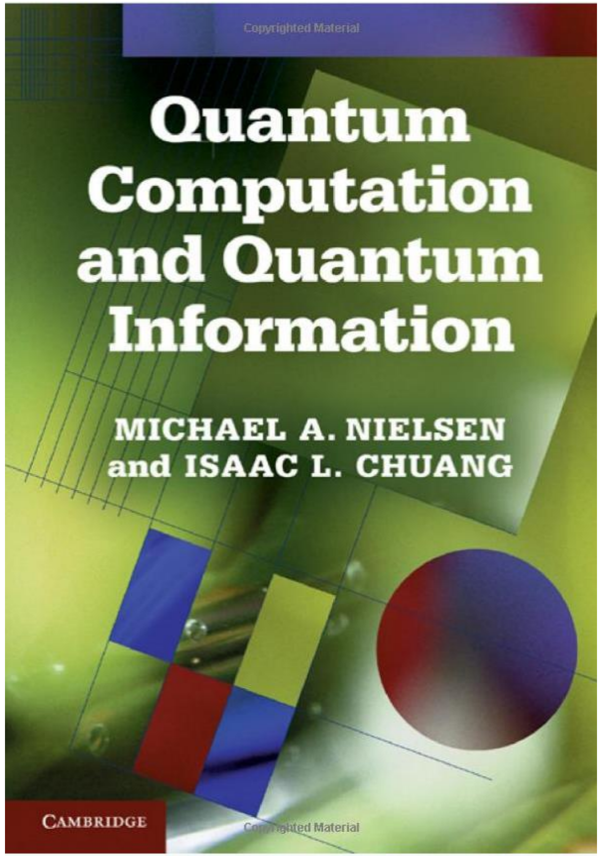
1. Qubits, States and Complexity
2. Challenges in Practice
3. An Interesting Algorithm for an HPC Workload
4. Outlook

Introduction to Quantum Computing

Paderborn Center for Parallel Computing

Disclaimers:

- I'm a **theoretical** physicist/chemist, so not a lot about experiments.
- This talk is very short, I had to throw in many grains of salt!
- This talk is focussed on **gate-based quantum computers** (Google, IBM,… but not D-Wave).
- **Great book**: Quantum Computation and Quantum Information, (Nielsen and Chuang)
- Experiments with QC:
    - https://quantum-computing.ibm.com/



Why Quantum Computers?

No efficient classical algorithms are known for many problems:

Factoring numbers:

3 x 7

=

21

Multiplication: simple

Factorization in prime numbers: still simple (for small numbers)

Paderborn Center for Parallel Computing

Why Quantum Computers?

No efficient classical algorithms are known for many problems:

Factoring numbers:

Multiplication: simple
1 ms on a single cpu-core

3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308773781446799948
9
x
36746043666799590428244633799627952632279158164343087642676032283815739666511279233373417143396810270092798736308917

=

12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434 13

$\in \mathcal{O}(2^k)$

Factorization in prime numbers:
HARD on classical computers!!!

768-bit RSA:

"2000 years of computing on a single-core 2.2 GHz AMD Opteron-based computer"

(https://eprint.iacr.org/2010/006.pdf)

- **BUT**: there is an **efficient <u>quantum</u> algorithm** to factor numbers:
  Shor's Algorithm by Peter Shor (*SIAM J. Comput.*, 26(5), 1484–1509., 1994)
  Complexity: $\in \mathcal{O}(k^3)$

Paderborn Center for Parallel Computing

Why Quantum Computers?

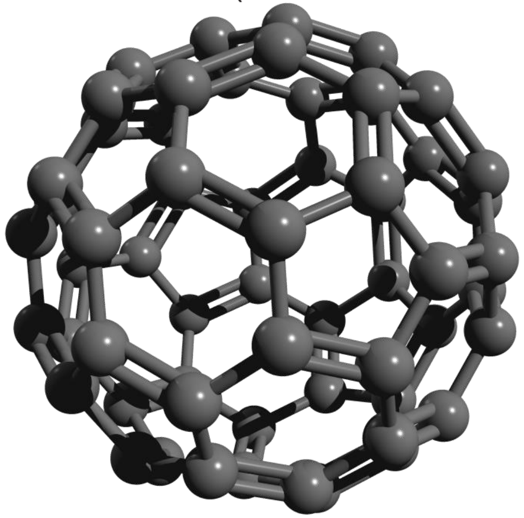
No efficient classical algorithms are known for many problems:

Quantum Chemistry, Solid-State Physics,…:

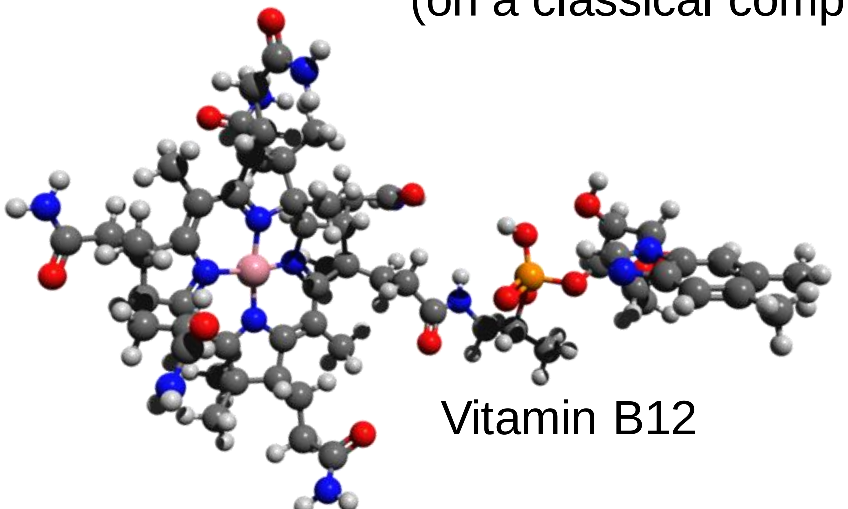
Challenge is to describe **quantum** systems (atoms, molecules, ...) on **classical** computers.

$$\left(\sum_i \frac{\hat{p}_i^2}{2m_e} + \sum_A \frac{\hat{P}_A^2}{2M_A} + \frac{1}{2}\sum_{i\neq j} \frac{e^2}{4\pi\epsilon_0 |\hat{r}_i - \hat{r}_j|} + \frac{1}{2}\sum_{A\neq B} \frac{e^2 Z_A Z_B}{4\pi\epsilon_0 |\hat{R}_A - \hat{R}_B|} - \frac{1}{2}\sum_{A,i} \frac{e^2 Z_A}{4\pi\epsilon_0 |\hat{R}_A - \hat{r}_i|} \right) |\Psi(t)\rangle = i\hbar\partial_t |\Psi(t)\rangle$$

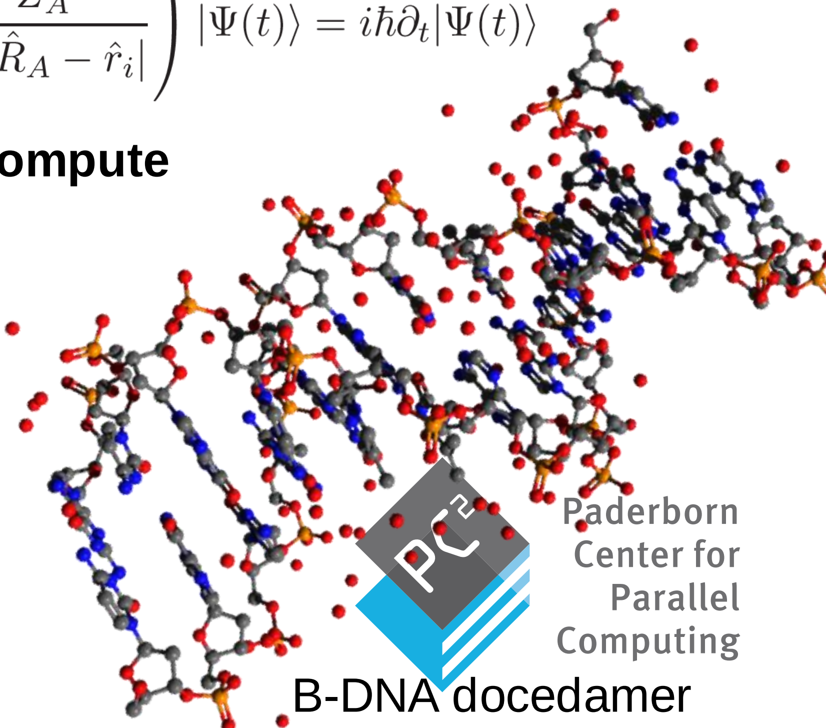
All basic physical laws are known, just **to hard to compute** (on a classical computer).



C60 Fullerene



Vitamin B12



B-DNA docedamer

Paderborn Center for Parallel Computing

Qubits, States and Complexity

Classical computer

Storage unit:

Bit

S=|0⟩ OR S=|1⟩

Qubits, States and Complexity

Classical computer

Storage unit:

Bit

$S=|0\rangle$ OR $S=|1\rangle$

Quantum computer

Storage unit:

Qubit

$S=|0\rangle$ $S=|1\rangle$

$$\mathbf{S=a|0\rangle+ b|1\rangle}$$

(a,b complex numbers, $1=a^2+b^2$)

A quantum system can be in **more than one** state at a time:
Superposition

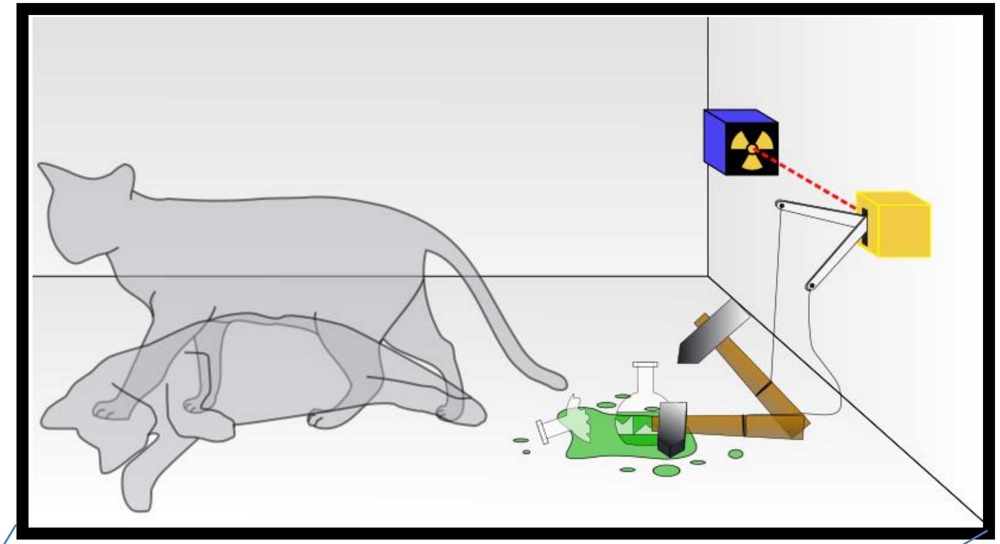
$S=|0\rangle + |1\rangle$:

- system is 50% in state $|0\rangle$ and 50% in state $|1\rangle$
  at the same time!

Paderborn Center for Parallel Computing

Superposition

Sketch by Dhatfield
(https://commons.wikimedia.org/wiki/File:Schrodingers_cat.svg)



S=|0⟩ + |1⟩:

- system is 50% in state |0⟩ and 50% in state |1⟩
  at the same time!

Schrodinger's cat (1935): thought experiment

Imagine a **cat in a closed box** with a poison:

- A random element (e.g. radioactive decay) controls the release of posion

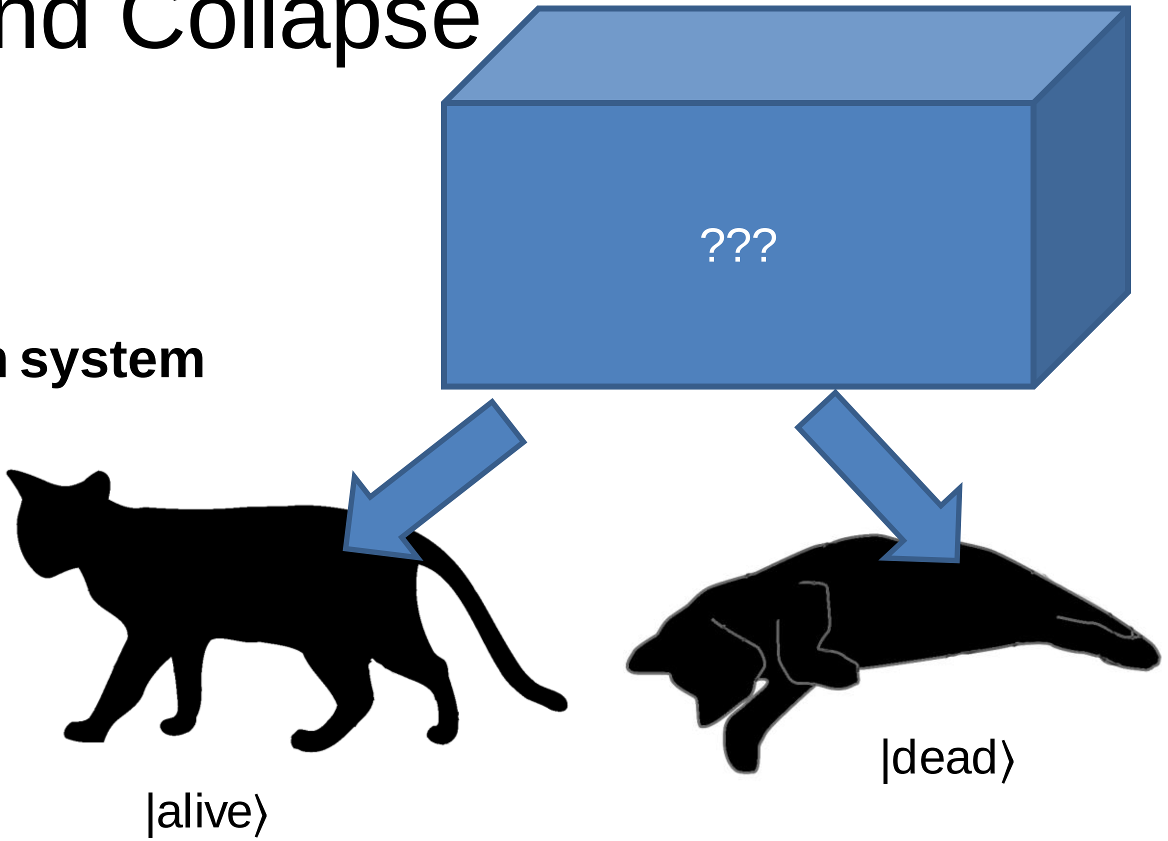
- The cat can be thought of as
  dead |dead⟩ and alive |alive⟩ at the same time!
  S_{cat}=|dead⟩+|alive⟩

Paderborn Center for Parallel Computing

Superposition and Collapse

$S_{cat}=|dead\rangle+|alive\rangle$

- As long as the box is closed, we don't know.
- When we open the box we **disturb the quantum system and the state collapses:**
  quantum-mechanical measurement



- **We measure**
  - with 50% probability |alive>
  - with 50% probability |dead>

(The collapse of the state is nothing magical, but can be described by quantum decoherence of a system (the box) interacting with the environment.)

Paderborn Center for Parallel Computing

Qubits, States and Complexity

<u>Classical computer</u>

Storage unit: **Bit**

$S=|0\rangle$ OR $S=|1\rangle$

Multiple storage units: N=8 bits

$S=|01011010\rangle$="Z"

$2^N=256$ different possibilities

A state is determined by **one integer number**.

Information stored = **N bits**

= 64 bit for N=64

<u>Quantum computer</u>

Qubits, States and Complexity

Classical computer

Storage unit: **Bit**

S=|0⟩ OR S=|1⟩

Multiple storage units: N=8 bits

S=|01011010⟩="Z"

2^N=256 different possibilities

A state is determined by **one integer number**.

Information stored = **N bits**
= 64 bit for N=64

Quantum computer

Storage unit: **Qubit**

S=|0⟩ S=|1⟩

S=a|0⟩+ b|1⟩

Multiple storage units: N=8 Qubits

$S=a_0|00000000\rangle+a_1|10000000\rangle+a_2|01000000\rangle+a_3|11000000\rangle+\dots$

A state is determined by an **exponential number (2^N) of complex numbers (a_0, a_1,…).**

Information stored = **2^N x 128 bit**
= **295148 PB** for 64 qubits

(assuming 64-bit double precision for the complex numbers)

Qubits, States and Complexity

Operations on quantum states:

S=a|0⟩ + b|1⟩ $\xrightarrow{\text{Op}}$ S'=Op(S)=a'|0⟩ + b'|1⟩

An operation Op maps a,b to a',b'

- Can be written as a **unitary transformation**, i.e., a 2x2 matrix U with $U^{-1}=(U^T)^*$

$$\begin{pmatrix} a' \\ b' \end{pmatrix} = U \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

Unitary ($U^{-1}=(U^T)^*$) because:

- Operation needs to be **reversible**
- Resulting state needs to be **normalized**, i.e. $a^2 + b^2 = 1 \quad \Rightarrow \quad a'^2 + b'^2 = 1$

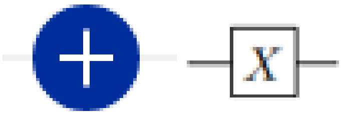
Very general, but hard to understand/imagine the operation.

Qubits, States and Complexity

Operations on quantum states:

Example: x-gate

$$U_\mathrm{x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



$$U_\mathrm{x}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} \quad \text{or} \quad U_x(a|0\rangle + b|1\rangle) = a|1\rangle + b|0\rangle$$

x-gate "switches" (flips) the qubit from $|0\rangle$ to $|1\rangle$ and vice versa.

name	unitary matrix	visual representation
Hadamard gate (h)	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$	$\lvert q_0\rangle$ H
σ_x gate (x)	$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$	$\lvert q_0\rangle$ X
σ_y gate (y)	$\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$	$\lvert q_0\rangle$ Y
σ_z gate (z)	$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$	$\lvert q_0\rangle$ Z
R_x gate (rx)	$e^{-i\theta\sigma_x/2} = \begin{pmatrix}\cos(\theta/2) & -i\sin(\theta/2)\\ -i\sin(\theta/2) & \cos(\theta/2)\end{pmatrix}$	$\lvert q_0\rangle$ $R_x(\theta)$
R_y gate (ry)	$e^{-i\theta\sigma_y/2} = \begin{pmatrix}\cos(\theta/2) & -\sin(\theta/2)\\ \sin(\theta/2) & \cos(\theta/2)\end{pmatrix}$	$\lvert q_0\rangle$ $R_y(\theta)$
R_z gate (rz)	$e^{-i\theta\sigma_z/2} = \begin{pmatrix}e^{-i\theta/2} & 0\\ 0 & e^{i\theta/2}\end{pmatrix}$	$\lvert q_0\rangle$ $R_z(\theta)$
phase shift	$e^{i\theta\mathbb{1}} = \begin{pmatrix}e^{i\theta} & 0\\ 0 & e^{i\theta}\end{pmatrix}$	$\lvert q_0\rangle$ $Ph(\theta)$
rotation gate (u3)	$\begin{pmatrix}e^{-i(\phi+\lambda)/2}\cos(\theta/2) & -e^{-i(\phi-\lambda)/2}\sin(\theta/2)\\ e^{i(\phi-\lambda)/2}\sin(\theta/2) & e^{i(\phi+\lambda)/2}\cos(\theta/2)\end{pmatrix}$	$\lvert q_0\rangle$ $U3(\theta,\phi,\lambda)$
phase gate (s)	$\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}$	$\lvert q_0\rangle$ S
phase gate† (sdag)	$\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}$	$\lvert q_0\rangle$ $S^\dagger$
swap gate	$\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}$	$\lvert q_0\rangle$ $\lvert q_1\rangle$
CNOT gate (cx)	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\lvert q_0\rangle$ $\lvert q_1\rangle$
Toffoli gate (cxx)	$\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{pmatrix}$	$\lvert q_0\rangle$ $\lvert q_1\rangle$ $\lvert q_2\rangle$

Qubits, States and Complexity

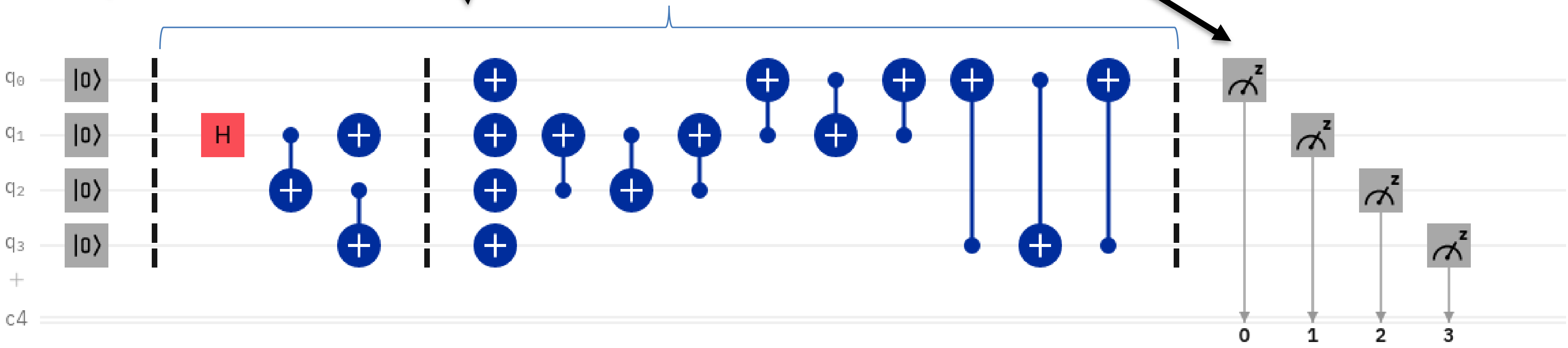
Operations on quantum states of multiple qubits: **Quantum Programs**

Build program from many small steps (quantum gates).

1. Start with a well-defined initial state, i.e., S=|00000000...⟩

2. Apply quantum gates to realise some operation.

3. Measure the probabilities.



https://quantum-computing.ibm.com/composer

Qubits, States and Complexity

Superposition for Computations:

3-qubit entangled state (GHZ-like)

$$(|0011\rangle - |0100\rangle)/\sqrt{2}$$

(7x) mod 15
modular multiplication

Resulting state is $(|0110\rangle - |1101\rangle)/\sqrt{2}$

We measure

- 0110 with 50% probability
- 1101 with 50% probability

state	x	(7x) mod 15	result
$\|0100\rangle$	4	13	$\|1101\rangle$
$\|0011\rangle$	3	6	$\|0110\rangle$

Superposition: apply one operation to many states at once!
Inherently parallel!

https://quantum-computing.ibm.com/composer

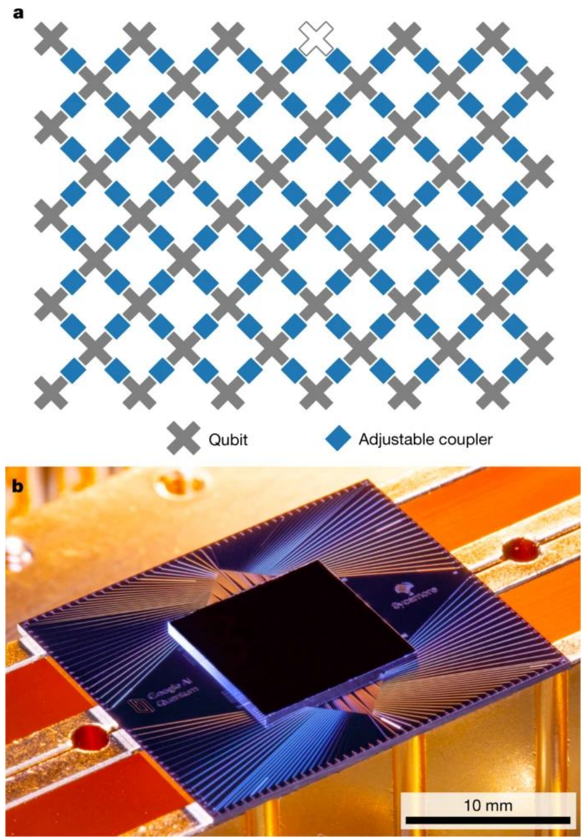
Challenges in Practice

- **Basic programming principles** and even some interesting algorithms known for several decades.

Requirements (DiVincenzo, Fortschr. Phys., 48: 771-783. 2000):

1. "a **scalable** physical system with well-characterized quantum-mechanical observables to represent the qubits,"

Sycamore quantum computer



Some physical principles of qubits:

- cooper pairs in Josephson junctions (e.g. transmon qubits)
- ions in electromagnetic traps manipulated with laser pulses,
- nuclear spins of molecules manipulated with nuclear magnetic resonance,
- single photons in non-linear optical media

Arute et al, [*Nature*] vol. 574, p. 505–510(2019)

Challenges in Practice

Requirements (DiVincenzo, Fortschr. Phys., 48: 771-783. 2000):

2. "a preparation of an **initial qubit state**,"

3. "a controllable unitary evolution with **single qubit-gates** and at least **one type of universal two-qubit gate"**

name	unitary matrix	visual representation
Hadamard gate (h)	$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$	$\lvert q_0\rangle$ — H —
σ_x gate (x)	$\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$	$\lvert q_0\rangle$ — X —
σ_y gate (y)	$\begin{pmatrix}0 & -i\\i & 0\end{pmatrix}$	$\lvert q_0\rangle$ — Y —
σ_z gate (z)	$\begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$	$\lvert q_0\rangle$ — Z —
R_x gate (rx)	$e^{-i\theta\sigma_x/2} = \begin{pmatrix}\cos(\theta/2) & -i\sin(\theta/2)\\-i\sin(\theta/2) & \cos(\theta/2)\end{pmatrix}$	$\lvert q_0\rangle$ — $R_x(\theta)$ —
R_y gate (ry)	$e^{-i\theta\sigma_y/2} = \begin{pmatrix}\cos(\theta/2) & -\sin(\theta/2)\\\sin(\theta/2) & \cos(\theta/2)\end{pmatrix}$	$\lvert q_0\rangle$ — $R_y(\theta)$ —
R_z gate (rz)	$e^{-i\theta\sigma_z/2} = \begin{pmatrix}e^{-i\theta/2} & 0\\0 & e^{i\theta/2}\end{pmatrix}$	$\lvert q_0\rangle$ — $R_z(\theta)$ —
phase shift	$e^{i\theta\mathbb{1}} = \begin{pmatrix}e^{i\theta} & 0\\0 & e^{i\theta}\end{pmatrix}$	$\lvert q_0\rangle$ — $Ph(\theta)$ —
rotation gate (u3)	$\begin{pmatrix}e^{-i(\phi+\lambda)/2}\cos(\theta/2) & -e^{-i(\phi-\lambda)/2}\sin(\theta/2)\\e^{i(\phi-\lambda)/2}\sin(\theta/2) & e^{i(\phi+\lambda)/2}\cos(\theta/2)\end{pmatrix}$	$\lvert q_0\rangle$ — $U3(\theta,\phi,\lambda)$ —
phase gate (s)	$\begin{pmatrix}1 & 0\\0 & i\end{pmatrix}$	$\lvert q_0\rangle$ — S —
phase gate† (sdag)	$\begin{pmatrix}1 & 0\\0 & -i\end{pmatrix}$	$\lvert q_0\rangle$ — $S^\dagger$ —
swap gate	$\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}$	$\lvert q_0\rangle$ — × — $\lvert q_1\rangle$ — × —
CNOT gate (cx)	$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$	$\lvert q_0\rangle$ — ● — $\lvert q_1\rangle$ — ⊕ —
Toffoli gate (cxx)	$\begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{pmatrix}$	$\lvert q_0\rangle$ — ● — $\lvert q_1\rangle$ — ● — $\lvert q_2\rangle$ — ⊕ —

Challenges in Practice

Requirements (DiVincenzo, Fortschr. Phys., 48: 771-783. 2000):

4. "**decoherence times** that are much longer than gate-operation times"

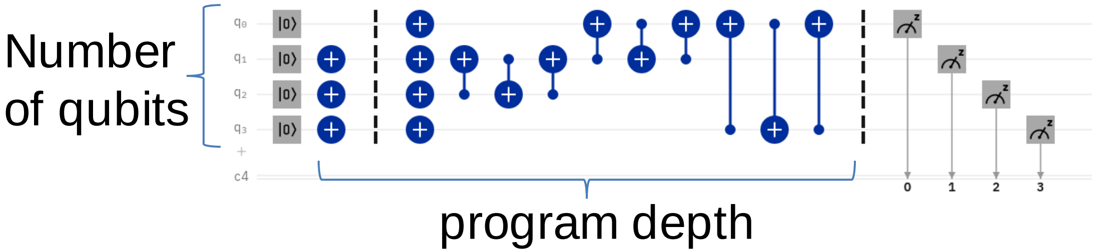
Decoherence time: The duration for which the quantum state can keep its **quantum nature**.
So basically the **time available to compute**.

- Noise from finite temperature
- Noise from external electric and magnetic fields
- Crosstalk between qubits
- …..

Challenges in Practice

Requirements (DiVincenzo, Fortschr. Phys., 48: 771-783. 2000):

4. **decoherence times** that are much longer than gate-operation times



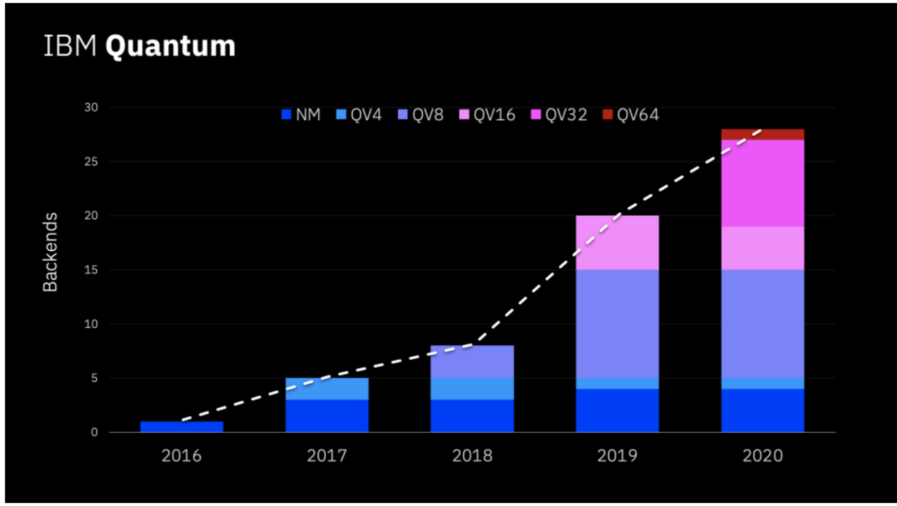
$$V \geq 4 \cdot 11 = 44$$

Power of a QC can be quantified with the **quantum volume V** (Moll, 2017):

- Number of qubits, decoherence times
- gate- and measurement error rates
- Connectivity of qubits

Example (with a grain of salt):

A value of V means that it can run any program where the product of **program depth and number of qubits** is smaller than V.



Source: IBM

An Interesting Algorithm for an HPC Workload

- Initially, most quantum algorithms assumed **perfect quantum computers.**
- Then **quantum error correction** schemes have been developed

  But **many qubits** needed and **long programs**.

New idea in the last ten years:

Simulate a quantum system (e.g. molecules) on quantum computers in a noise-tolerant way.

An Interesting Algorithm for an HPC Workload

<u>Quantum computer</u>

New idea in the last ten years:

Simulate a quantum system (e.g. molecules) on quantum computers in a noise-tolerant way.

Variational Classical Eigensolvers

(VASP, CP2K, Gaussian,…)

$$E_{GS} = \min_{\vec{x}} E(\Psi(\vec{x}))$$

i.e. minimize the energy to find the ground state.

* Note: depending on the level of theory (DFT, CCSD(T),…) the wave functions are single-particle wave functions or many-particle wave functions.

An Interesting Algorithm for an HPC Workload

New idea in the last ten years:

Simulate a quantum system (e.g. molecules) on quantum computers in a noise-tolerant way.

Variational Classical Eigensolvers

(VASP, CP2K, Gaussian,…)

$$E_{GS} = \min_{\vec{x}} E(\Psi(\vec{x}))$$

i.e. minimize the energy to find the ground state.

Quantum computer

Variational Quantum Eigensolver (VQE)

(VQE, Peruzzo et. al, 2013)

$$E_{GS} = \min_{\vec{x}} E(\Psi(\vec{x}))$$

i.e. minimize the energy to find the ground state.
Parameters are optimized on the classical computer.

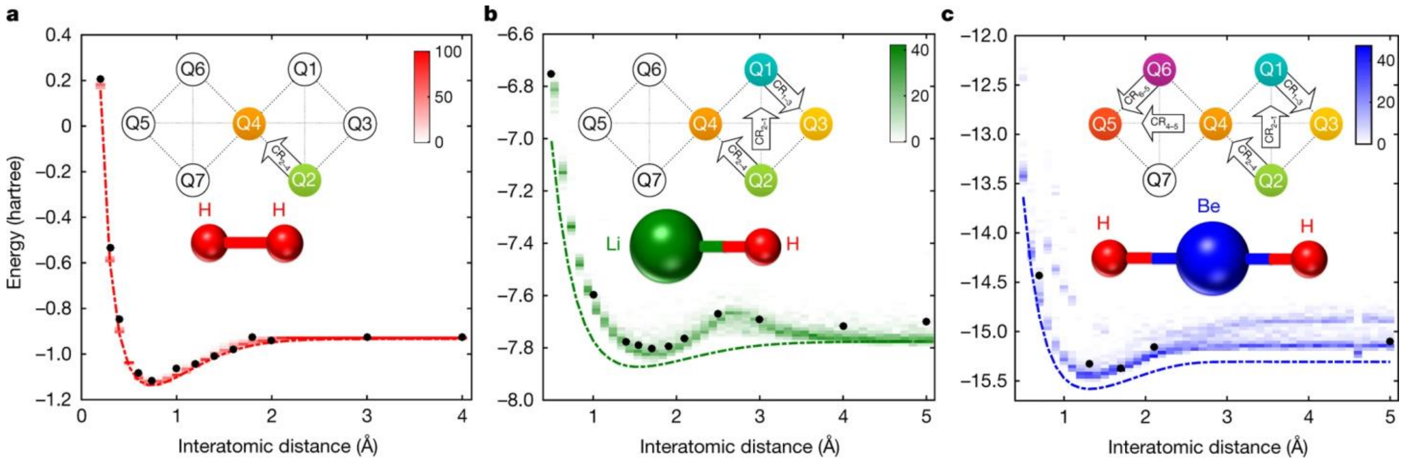
BUT: Energy is calculated on the QC!

- automatically compensates crosstalk and shifts
- **noise-tolerant***
- Even 35-100 qubits can give results that no supercomputer can.

* Note: depending on the level of theory (DFT, CCSD(T),…) the wave functions are single-particle wave functions or many-particle wave functions.

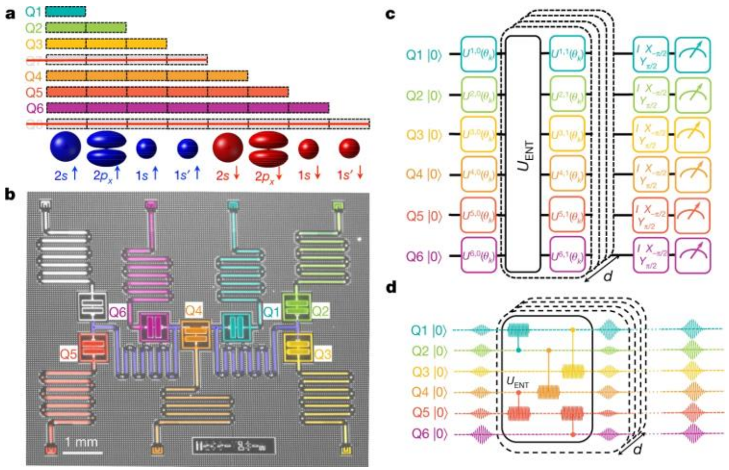
An Interesting Algorithm for an HPC Workload

Variational Quantum Eigensolver (VQE, Peruzzo et. al, 2013):



Kandala et. al, [*Nature*]() **vol. 549**, p. 242–246 (2017)

$$E_{GS} = \min_{\vec{x}} E(\Psi(\vec{x}))$$



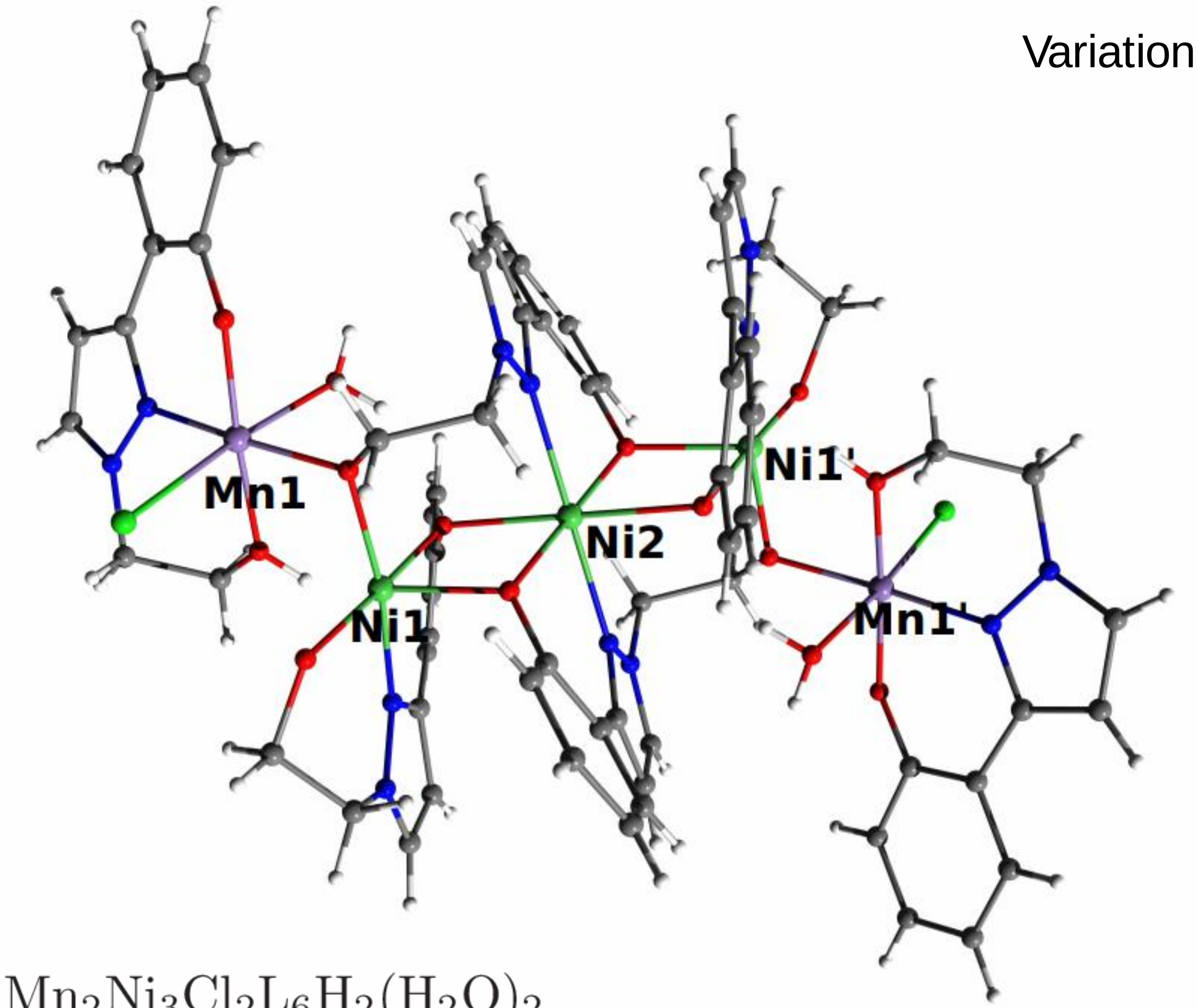
i.e. minimize the energy to find the ground state.

BUT: Energy is calculated on the QC!

- automatically compensates crosstalk and shifts
- **noise-tolerant***
- Even 35-100 qubits can give results that no supercomputer can.

An Interesting Algorithm for an HPC Workload

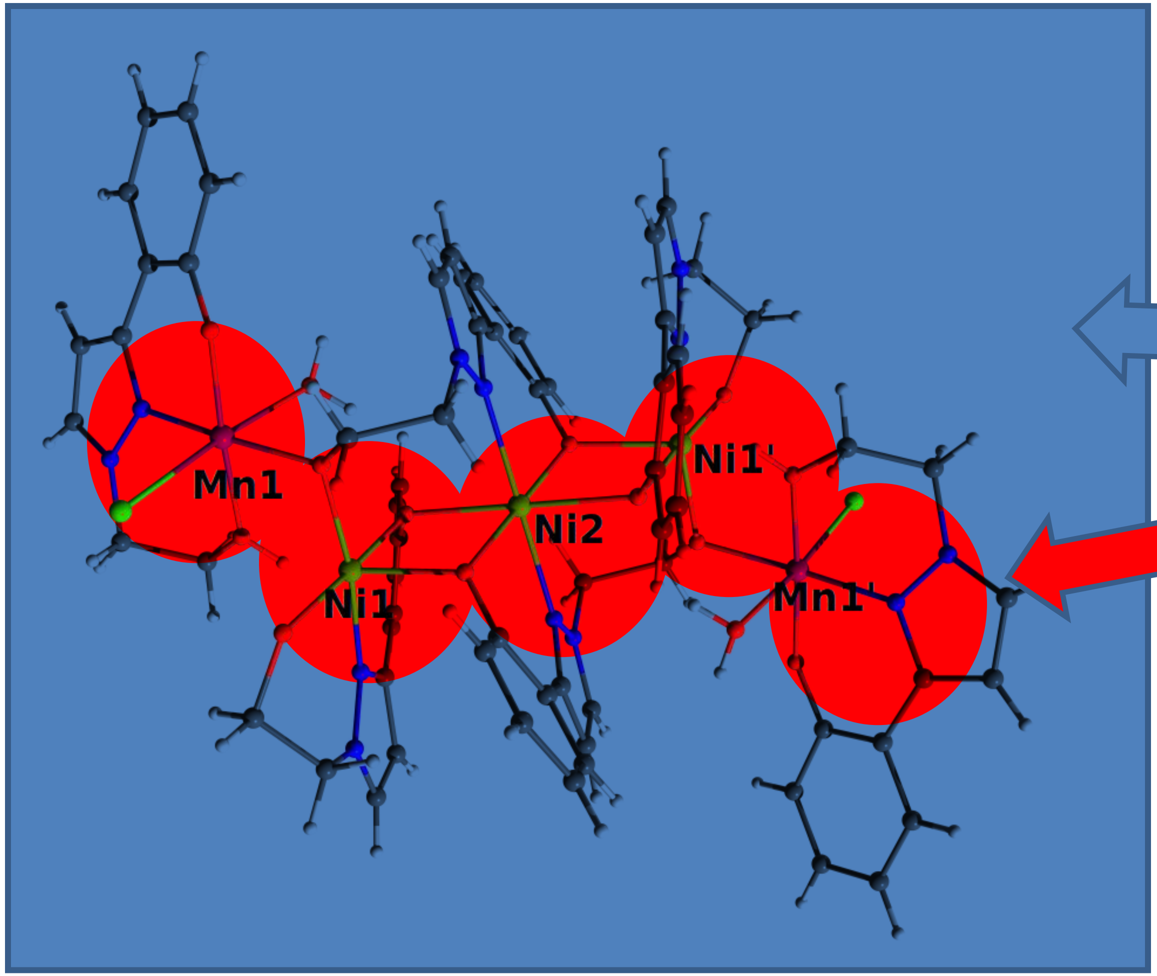
Variational Quantum Eigensolver: ~500 qubits required



$Mn_2Ni_3Cl_2L_6H_2(H_2O)_2$

Das et al., *J. Am. Chem. Soc.* 2011, 133, 10, 3433–3443

An Interesting Algorithm for an HPC Workload



Variational Quantum Eigensolver: ~500 qubits required

Idea: decompose the molecule

Outer part: Treated with approx. DFT methods on a classical computer (cubic or linear scaling)

Inner part: Treated with VQE-like algorithm on QC requires only ~90 qubits

Decomposition can be performed consistently based on the reduced density-matrix functional

Decomposition: Schade et al, EPJ ST **226**, 2677 (2017)
Solution of inner part on QC: Schade et al. in preparation, initial results in 10.5281/zenodo.4022026

$\mathrm{Mn_2Ni_3Cl_2L_6H_2(H_2O)_2}$

Das et al., *J. Am. Chem. Soc.* 2011, 133, 10, 3433–3443

Outlook

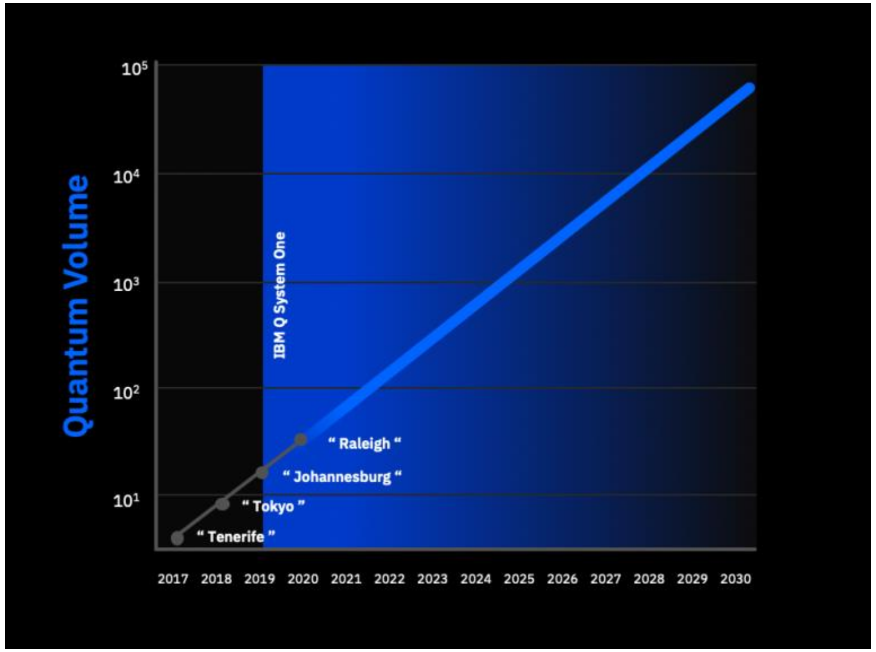
- Hopefully an **exponential increase** in quantum volume.
- An interesting race to increase quantum volume. (Many big players: IBM, Google, Microsoft, Rigetti, …

- Thankfully, **post-quantum cryptography** is already well developed.
- Quantum supremacy for useful workloads is only a matter of time.

- Creativity: Many new clever algorithms expected.

- **Chemistry / Physics / Biology**:
  - Most of the algorithmic developments of the last 90 years have to be thrown away.
  - But many new oportunities for hybrid-quantum-classical algorithms.
  - Probably some real HPC workloads run on QCs by 2030.

- Unfortunately a lot of buzzword-bingo to come: "Quantum AI"



Source: https://www.ibm.com/blogs/research/2020/01/quantum-volume-32/