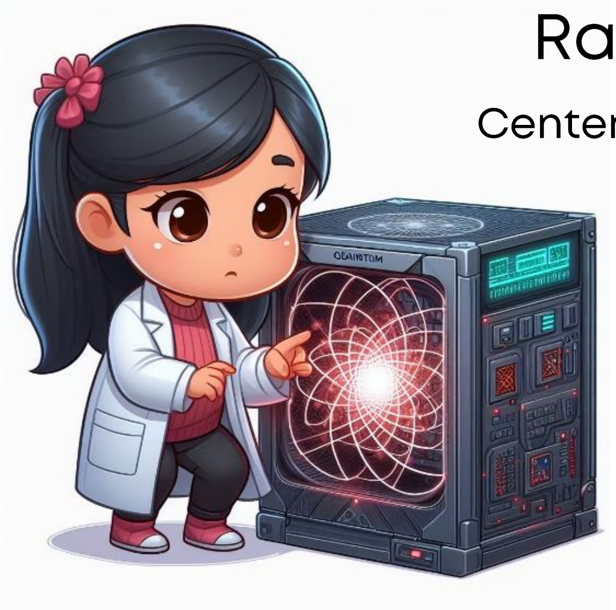
RaTSIf-2023a

Quantum Computing:

Advancements and Challenges



Raqueline A. M. Santos

Center for Quantum Computer Science

University of Latvia

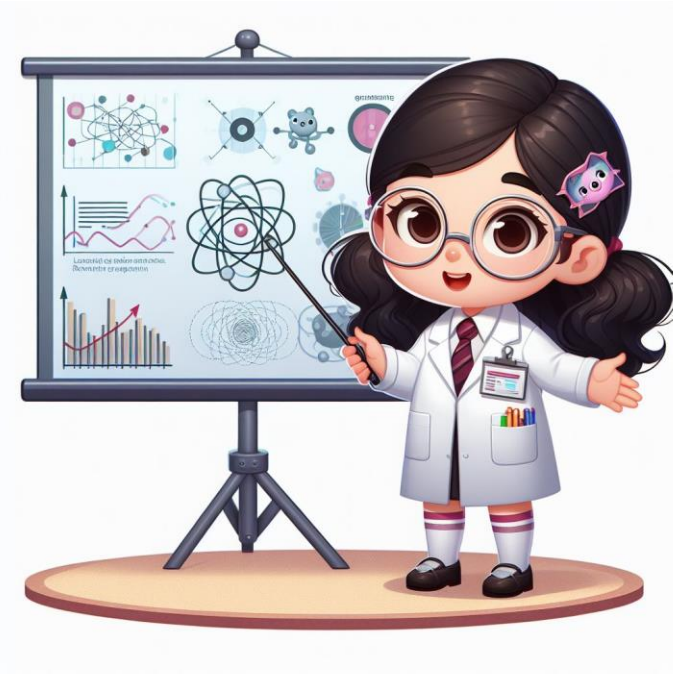
Latvian Quantum Initiative

Funded by the European Union NextGenerationEU

2027 National Development Plan

Summary

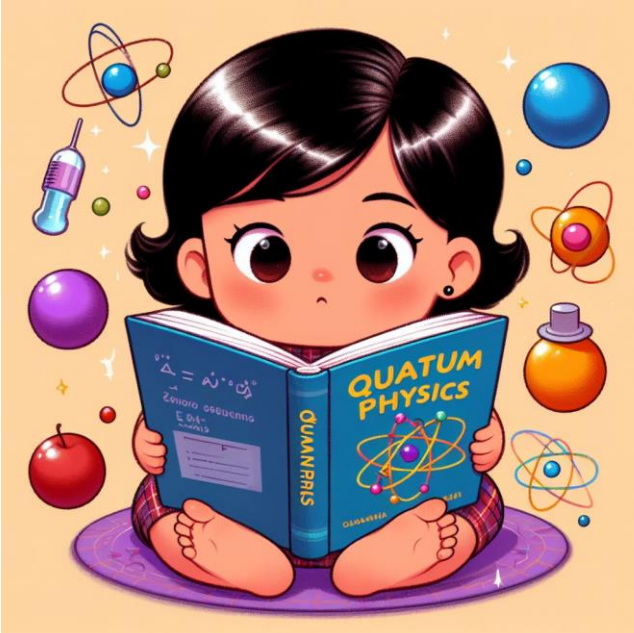
- Why is quantum different?
- Quantum algorithms
- Potential Applications
- Building a quantum computer
- What do we have so far?



Latvian Quantum Initiative
Funded by the European Union
NextGenerationEU
2027 National Development Plan

Why is quantum different?

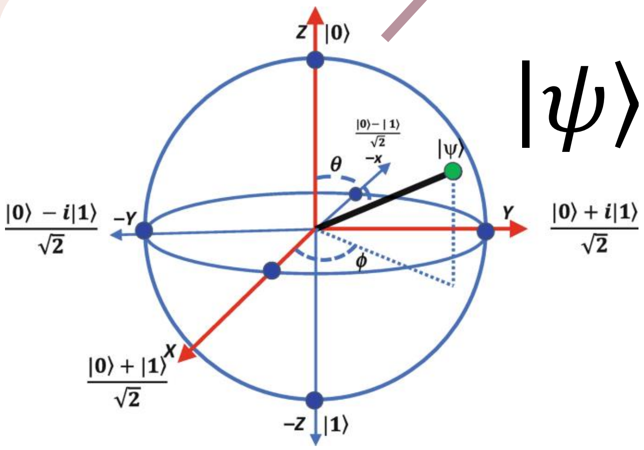
- 1982 – Richard Feynman
  - creating a machine based on the laws of quantum mechanics
- Quantum Physics is the theory that describes the smallest particles, like electrons and atoms.
- Quantum allows us to perform certain processes in a fundamentally different way.
  - quantum computers do not make existing software run faster. They run quantum algorithms.
- Bits vs Quantum bits (qubits).



Why is quantum different?

- Superposition
- Entanglement
- Interference

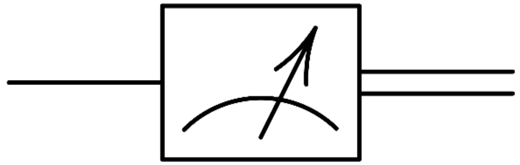
Bloch sphere (qubit representation)



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha, \beta \in \mathbb{C}$$

$|\psi\rangle$



$$|0\rangle: |\alpha|^2$$

$$|1\rangle: |\beta|^2$$

$$|\alpha|^2 + |\beta|^2 = 1$$

Latvian Quantum Initiative
Funded by the European Union
NextGenerationEU
2027 National Development Plan

Why is quantum different?

- Superposition
- Entanglement
- Interference

2- qubit system

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \eta|11\rangle$$

n- qubit system

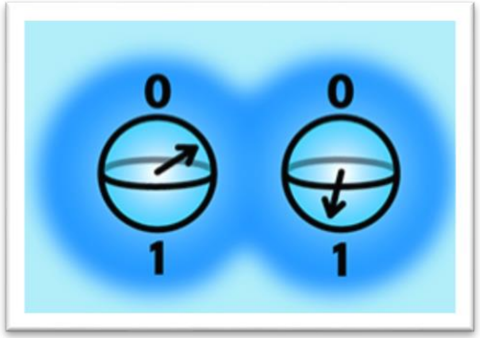
Superposition of 2^n states

Latvian Quantum Initiative
Funded by the European Union
NextGenerationEU
2027 National Development Plan

Why is quantum different?

- Superposition
- Entanglement
- Interference

Multiple qubits can exhibit quantum entanglement



*Domain of Science
https://www.flickr.com/photos/95869671@N08/

The quantum state of each particle of the group cannot be described independently of the state of the others (including when the particles are separated by a large distance!)

Why is quantum different?

- Superposition
- Entanglement
- Interference

1. $$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Not entangled

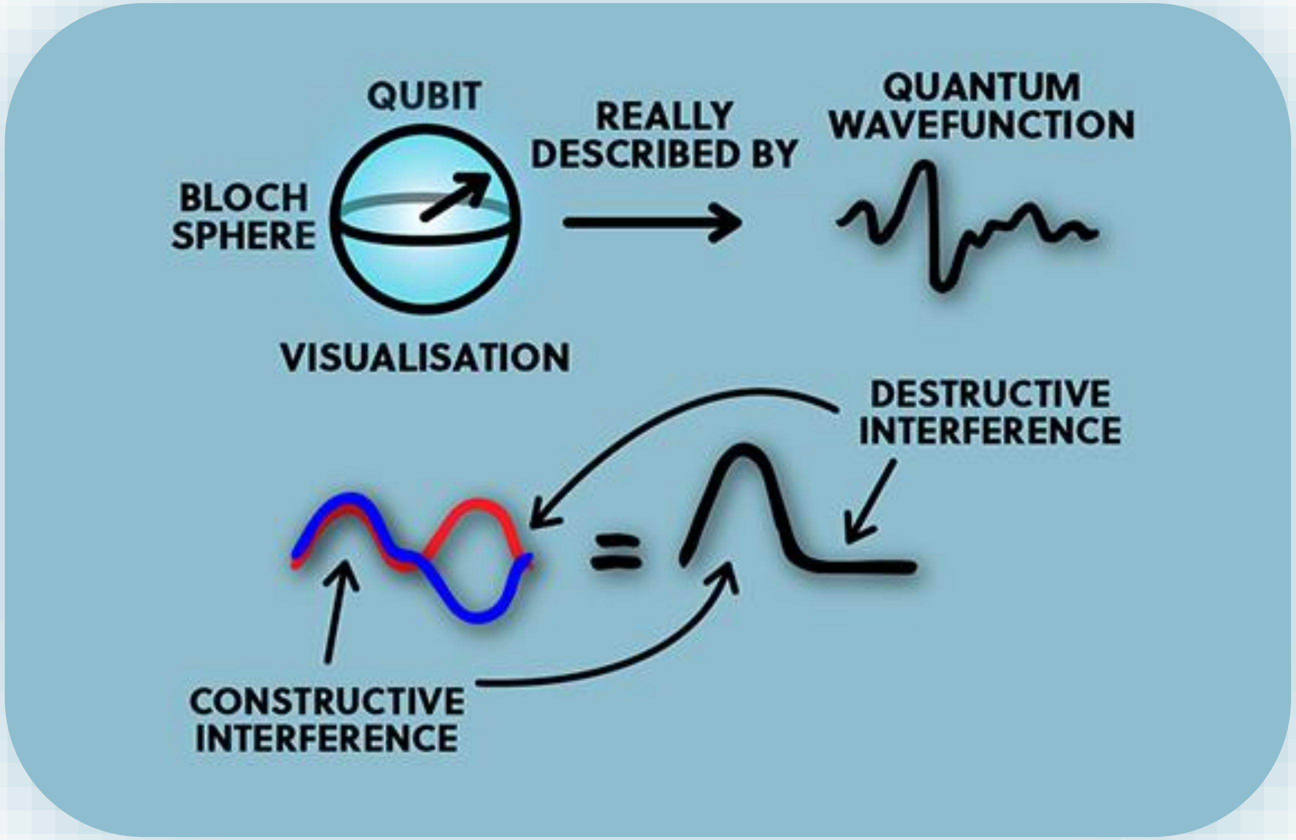
2. $$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

Entangled

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

Why is quantum different?

- Superposition
- Entanglement
- Interference

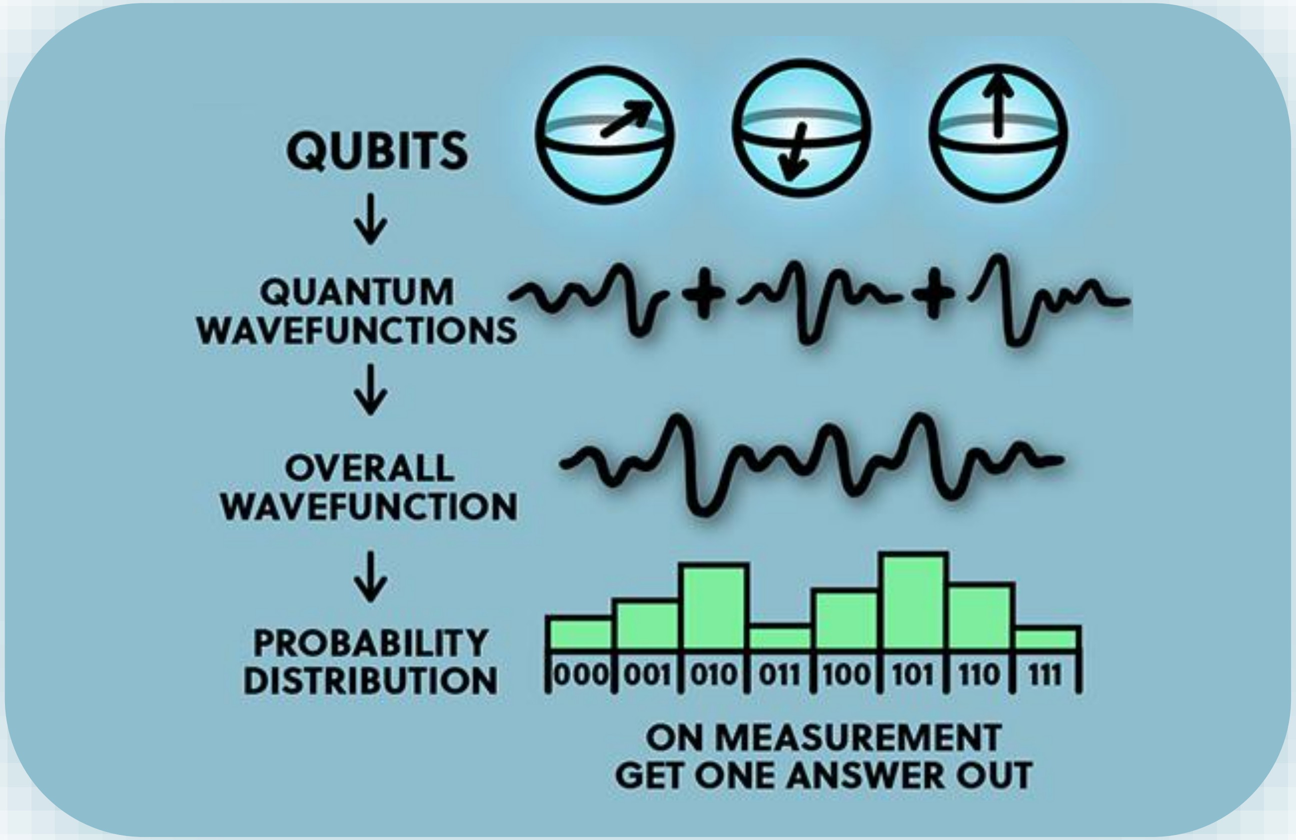


*Domain of Science https://www.flickr.com/photos/95869671@N08/

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

Why is quantum different?

- Superposition
- Entanglement
- Interference



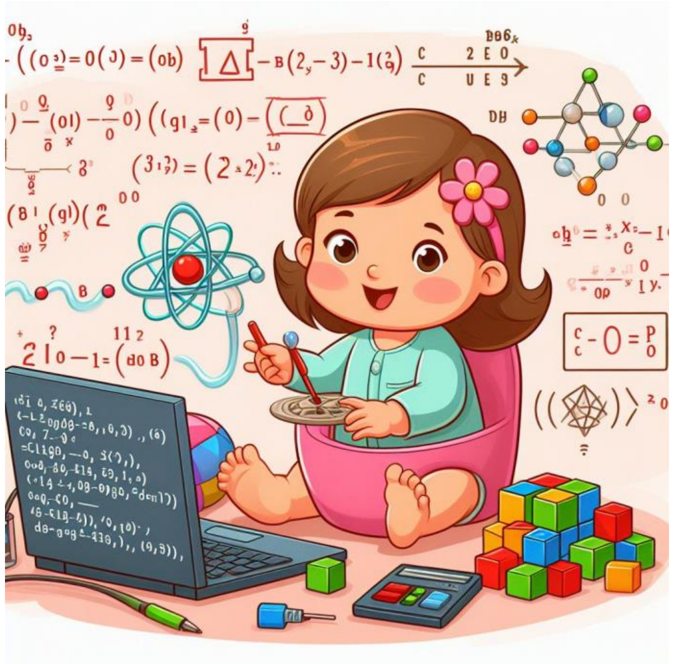
*Domain of Science https://www.flickr.com/photos/95869671@N08/

Why is quantum different?

- Superposition
- Entanglement
- Interference

Essential in the role of designing quantum algorithms

Quantum algorithms



- Shor's algorithm
- Grover's algorithm
- Quantum search by quantum walks

Quantum algorithms

Shor (1994)

- Polynomial time algorithm for factoring integers and finding discrete logarithms
- Exponential speed-up compared to the best known classical algorithm
- Significant threat to the cryptography methods widely used today

- Shor's algorithm
- Grover's algorithm
- Quantum search by quantum walks

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

Quantum algorithms

Grover (1996)

- Quantum algorithm for searching an unsorted database with N entries in $O(\sqrt{N})$ steps.
- Classically, it requires $O(N)$ steps

- Shor's algorithm
- Grover's algorithm
- Quantum search by quantum walks

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

Quantum algorithms

Ambainis, Gilyen, Jeffery, Kokainis (2020)

- Quantum algorithm for finding a marked vertex in any graph, with any set of marked vertices.
- (up to a log factor) quadratically faster than the corresponding classical random walk
- Resolved a question that had been open for 15 years.

- Shor's algorithm
- Grover's algorithm
- Quantum search by quantum walks

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

Potential Applications

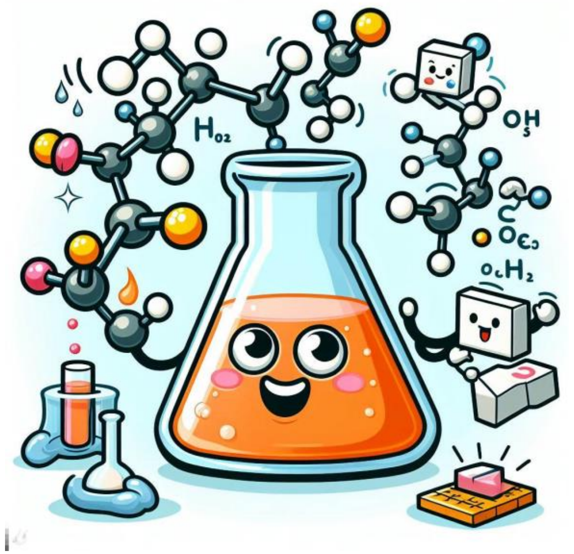
- Some problems can profit greatly from a quantum computer, whereas many won't
- Not suited for most everyday processing (better use the classical computer!)

Potential Applications

- Some problems can profit greatly from a quantum computer, whereas many won’t
- Not suited for most everyday processing (better use the classical computer!)

Quantum Simulation

- Simulation of other quantum systems and materials
- Designing new chemical process
- Estimating effects of new medicines
- Applications in condensed-matter physics, cosmology, etc.



Potential Applications

Break certain types of cryptography

- Shor's algorithm can break the RSA (and other public key cryptographic systems)
  - Based on integer factorization of big numbers
  - A plausible quantum computer could factor a 2048-bit number in about 8 hours using 20 million noisy qubits.

Quantum
the open journal for quantum science
PAPERS PERSPECTIVES

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2,3]

[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[3]Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

Published: 2021-04-15, volume 5, page 433
Eprint: arXiv:1905.09749v3
Doi: https://doi.org/10.22331/q-2021-04-15-433
Citation: Quantum 5, 433 (2021).

Potential Applications

Break certain types of cryptography

- Shor's algorithm can break the RSA (and other public key cryptographic systems)
  - Based on integer factorization of big numbers
  - A plausible quantum computer could factor a 2048-bit number in about 8 hours using 20 million noisy qubits.

⟨Quantum
the open journal for quantum science

PAPERS PERSPECTIVES

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2,3]

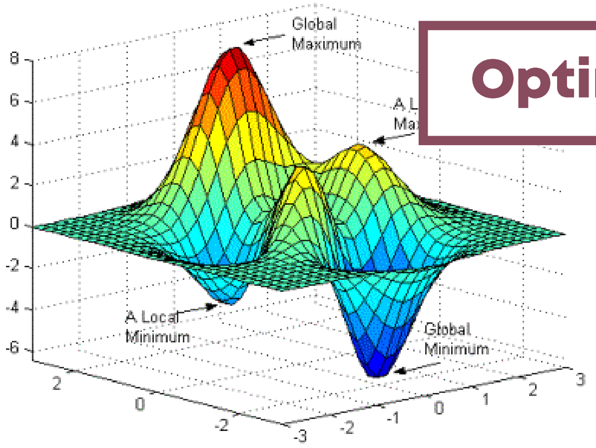
[1]Google Inc., Santa Barbara, California 93117, USA
[2]KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
[3]Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

Published:	2021-04-15, volume 5, page 433
Eprint:	arXiv:1905.09749v3
Doi:	https://doi.org/10.22331/q-2021-04-15-433
Citation:	Quantum 5, 433 (2021).

- **Luckily, not all cryptography is broken!**
- Post-quantum Cryptography
- Quantum cryptography (QKD)

NextGenerationEU
National Development Plan

Potential Applications

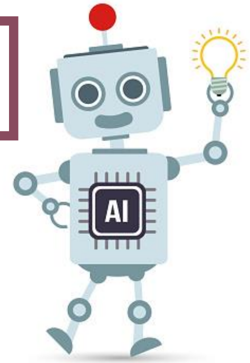


Optimization problems

Weather forecast

Financial modelling

Machine learning and AI



Latvian Quantum Initiative

Funded by the European Union NextGenerationEU

2027 National Development Plan

Building a Quantum Computer

Models of Quantum Computing

- Quantum circuit model
- Measurement-based quantum computing
- Adiabatic quantum computing
- Topological quantum computing
- Quantum Turing machine

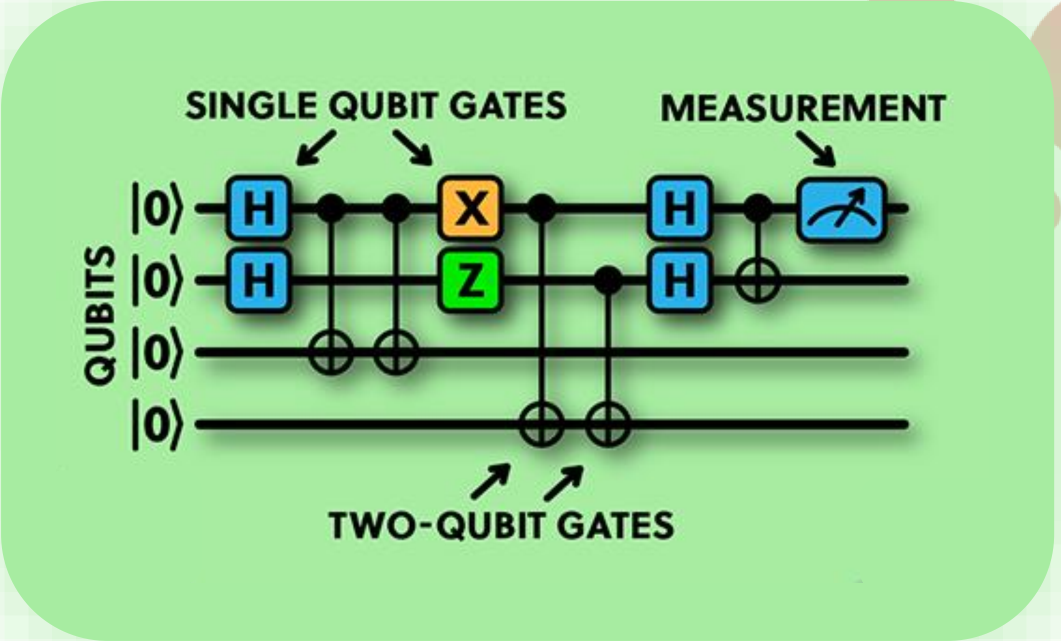
- Quantum annealing (not universal)

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

Building a Quantum Computer

Quantum Circuit Model

- A quantum computation is decomposed into a sequence of quantum logic gates and measurements.



*from Domain of Science https://www.flickr.com/photos/95869671@N08/

Latvian Quantum Initiative

Funded by the European Union
NextGenerationEU

2027 National Development Plan

Building a Quantum Computer

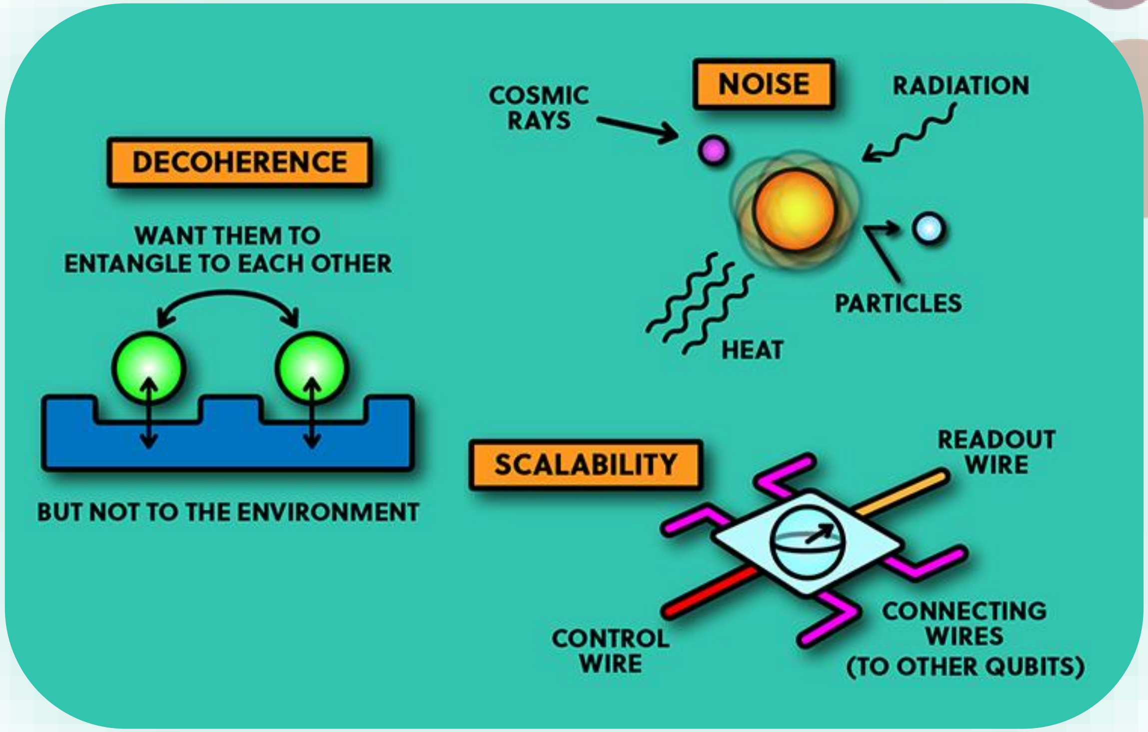
Physical Implementation

- There are many different quantum systems that you can potentially build them from.
- Qubit: two-state quantum system
  - Spin of a particle…
- No matter what the approach is, they all face some obstacles

Building a Quantum Computer

Challenges

- Decoherence
  - is the loss of quantum coherence, which can happen by any slight interaction with the outside world.
- Noise
  - You have to protect the qubits from any kind of noise: cosmic rays, heat radiation, rogue particles…
- Scalability
  - Any quantum computer design needs to somehow be able to entangle all of the qubits, and then control and measure them in a scalable way.

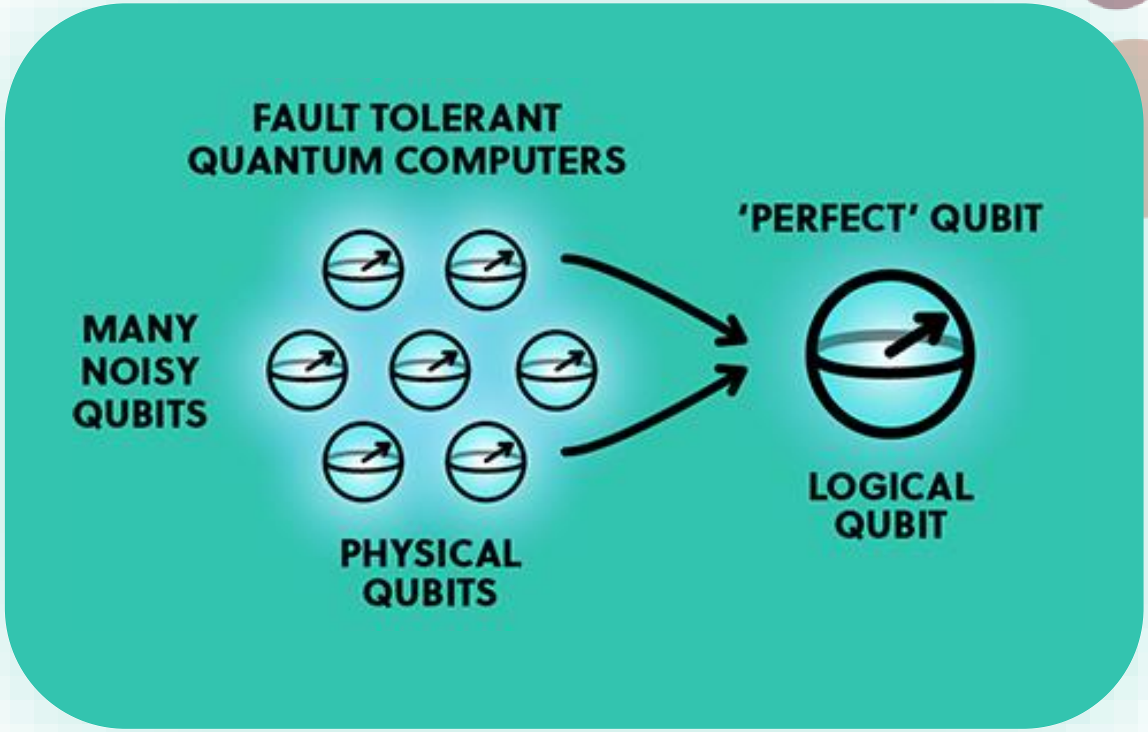


*Domain of Science https://www.flickr.com/photos/95869671@N08/

Building a Quantum Computer

Quantum error correction

- Use of many noisy qubits together to represent a noise free qubit (logical qubit)
- How many do we need?
  - Depends on the implementation of the physical qubits
  - Estimation: around 100 to 1000 qubits to make one fault-tolerant qubit



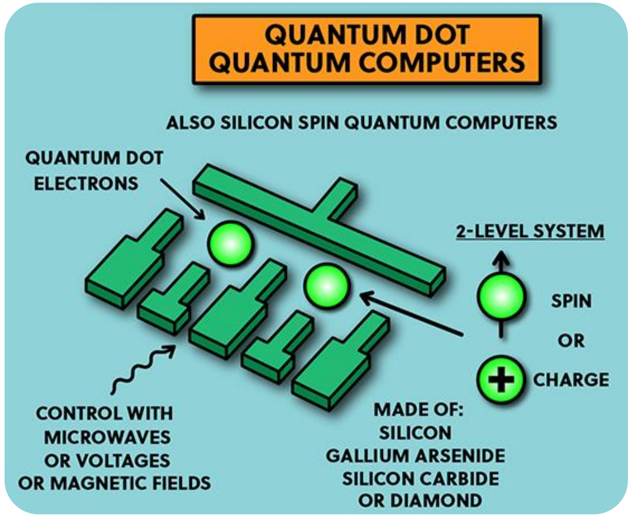
*Domain of Science https://www.flickr.com/photos/95869671@N08/

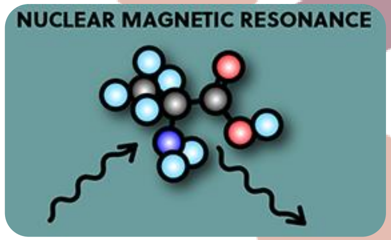
Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

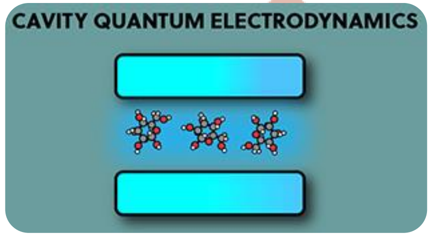
Building a Quantum Computer

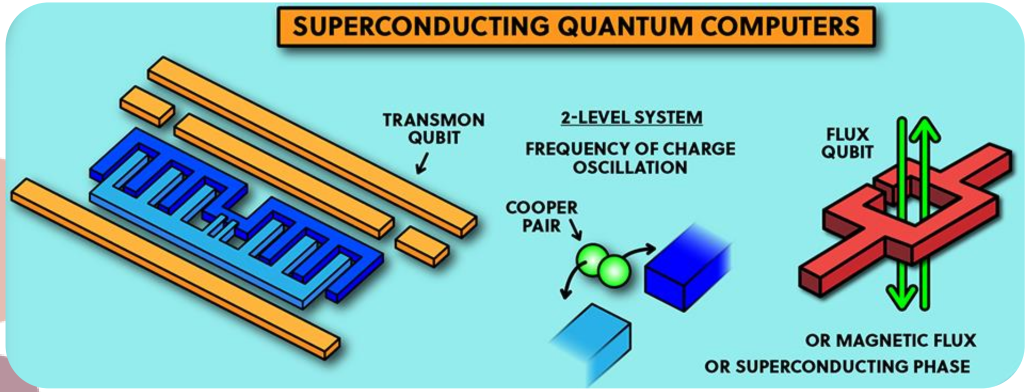
Qubit technologies

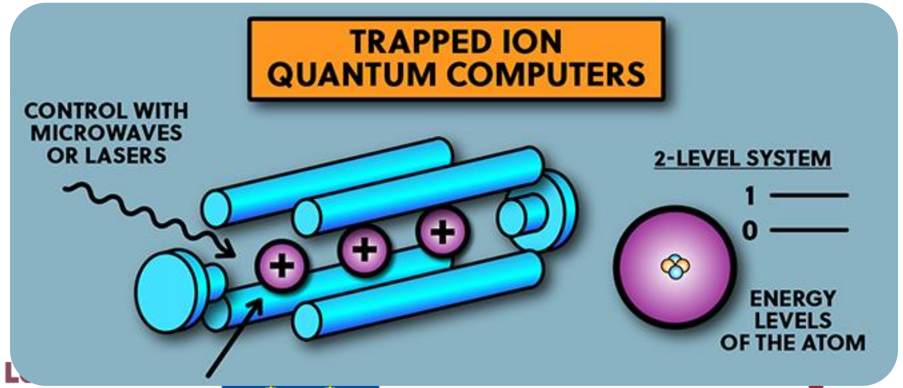
- Superconducting qubits (e.g. IBM)
- Trapped-ion qubits (e.g. IonQ)
- Photonic qubits (e.g. Xanadu)
- Silicon spin qubits in quantum dots (e.g. Intel)
- Neutral atom qubits (e.g. Atom Computing)
- Topological qubits (e.g. Microsoft)









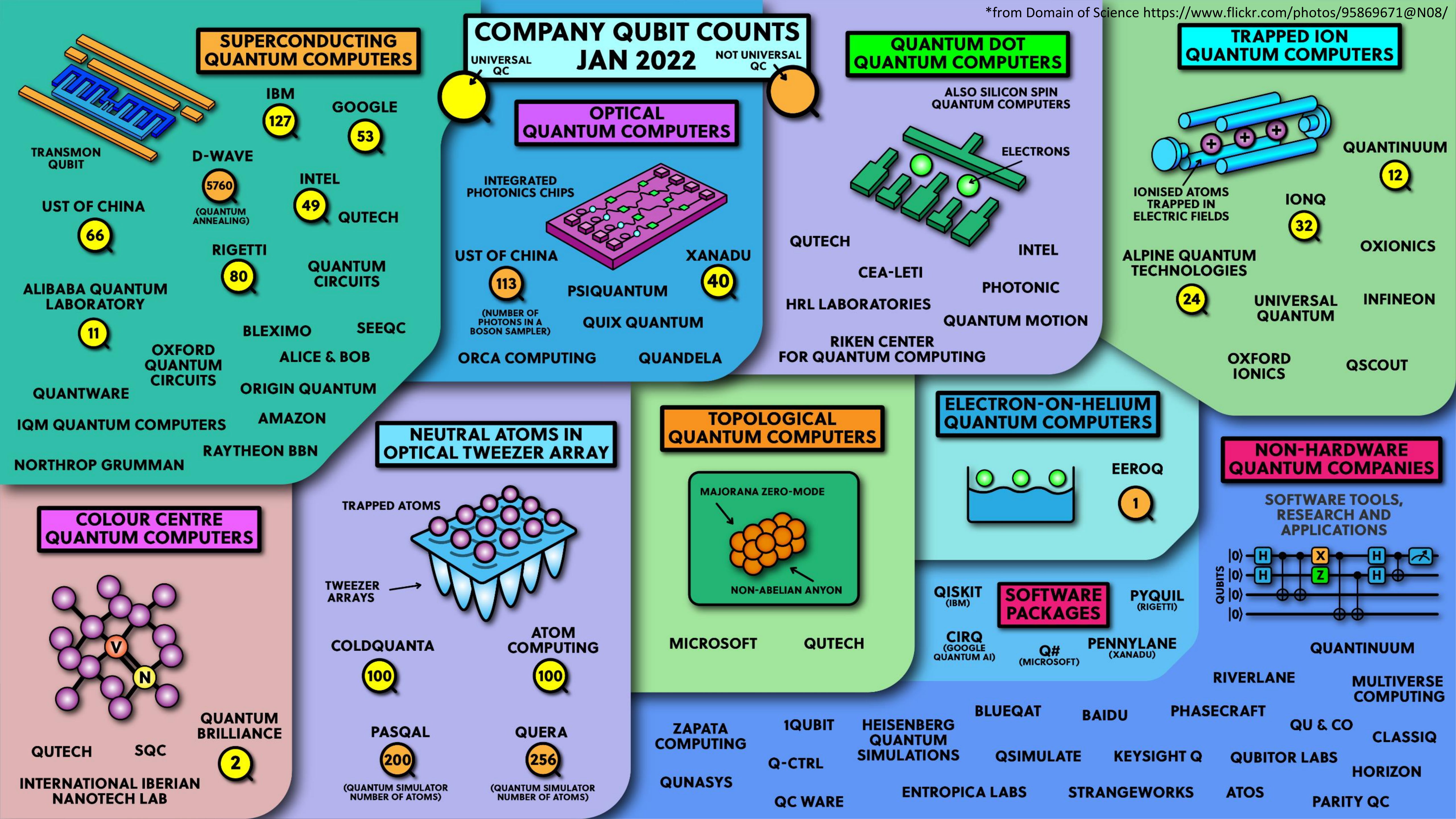


*Domain of Science https://www.flickr.com/photos/95869671@N08/

What do we have so far?

- NISQ era (Noisy Intermediate Scale Quantum)
  - Term coined by John Preskill in 2018
  - Small quantum computers not yet capable of large-scale error correction
  - Many are in principle universal, except that they are limited both in the number of qubits, and in the number of steps that can be executed.

- In the past few years many companies have been investing in quantum computing and trying to build one.



*from Domain of Science https://www.flickr.com/photos/95869671@N08/

Circuit based

Company	Architecture	#Qubits	Date
Alpine Quantum Technologies	Trapped Ion	24	2021
Atom Computing	Neutral atoms in optical lattices	100	2021
Google	Superconducting transmon	53	2019
IBM	Superconducting	433	2022
Intel	Superconducting	49	2018
IonQ	Trapped Ion	32	2022
Quantinum	Trapped Ion	32	2023
Rigetti	Superconducting transmon	80	2022
Xanadu	Photonics	216	2022
D-Wave	Superconducting	5760	2020

Quantum annealling

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

What do we have so far?

Quantum Volume

- Metric that measures the capabilities and error rates of a quantum computer
- It can compare many different architectures (universal quantum computers)
- Requires a set of statistical tests
  - Number of qubits
  - Error rates
  - Connectivity of qubits
- Generally, the larger the quantum volume, the more complex the problems a quantum computer can solve

Latvian Quantum Initiative
Funded by the European Union
NextGenerationEU
2027 National Development Plan

What do we have so far?

Quantum Volume

- If a processor has a Quantum Volume of 2^N, it means that the device is likely to produce the right output of a square quantum circuit on some subset of N qubits with N layers of random two-qubit gates.

Date	Quantum Volume	Manufacturer	#Qubits
2022, April	256 (2^8)	IBM	27
2022, April	4096 (2^{12})	Quantinuum	12
2022, May	512 (2^9)	IBM	27
2022, September	8192 (2^{13})	Quantinuum	20
2023, February	128 (2^7)	Alpine Quantum Technologies	24
2023, February	32,768 (2^{15})	Quantinuum	20
2023, May	65,536 (2^{16})	Quantinuum	32
2023, June	524,288 (2^{19})	Quantinuum	20

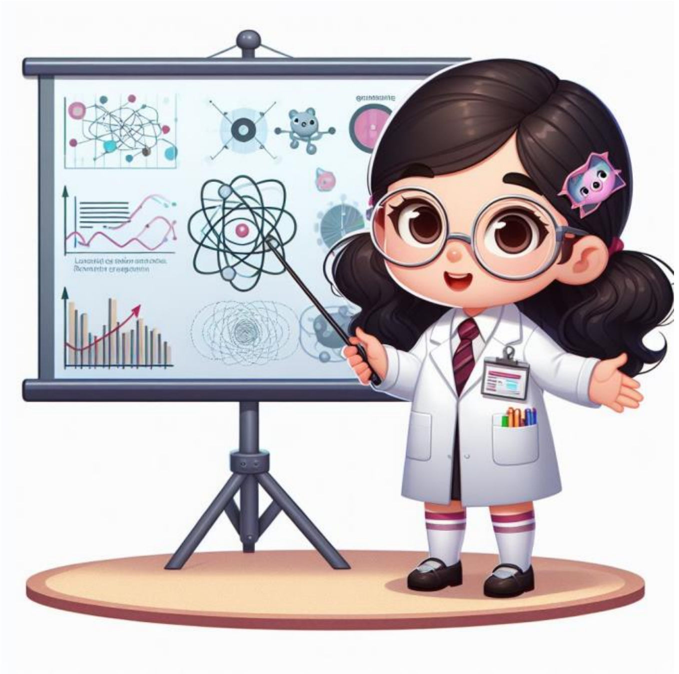
What do we have so far?

- We will need other metrics in the future
  - Calculating the quantum volume needs classical simulations (will be impossible when quantum computers become large)
  - Quantum volume doesn't take into account the time to solve a problem
  - CLOPS – Circuit Layer Operations Per Second (quantum version of FLOPS)
  - EPLG – Error Per Layered Gate

Latvian Quantum Initiative
Funded by the European Union NextGenerationEU
2027 National Development Plan

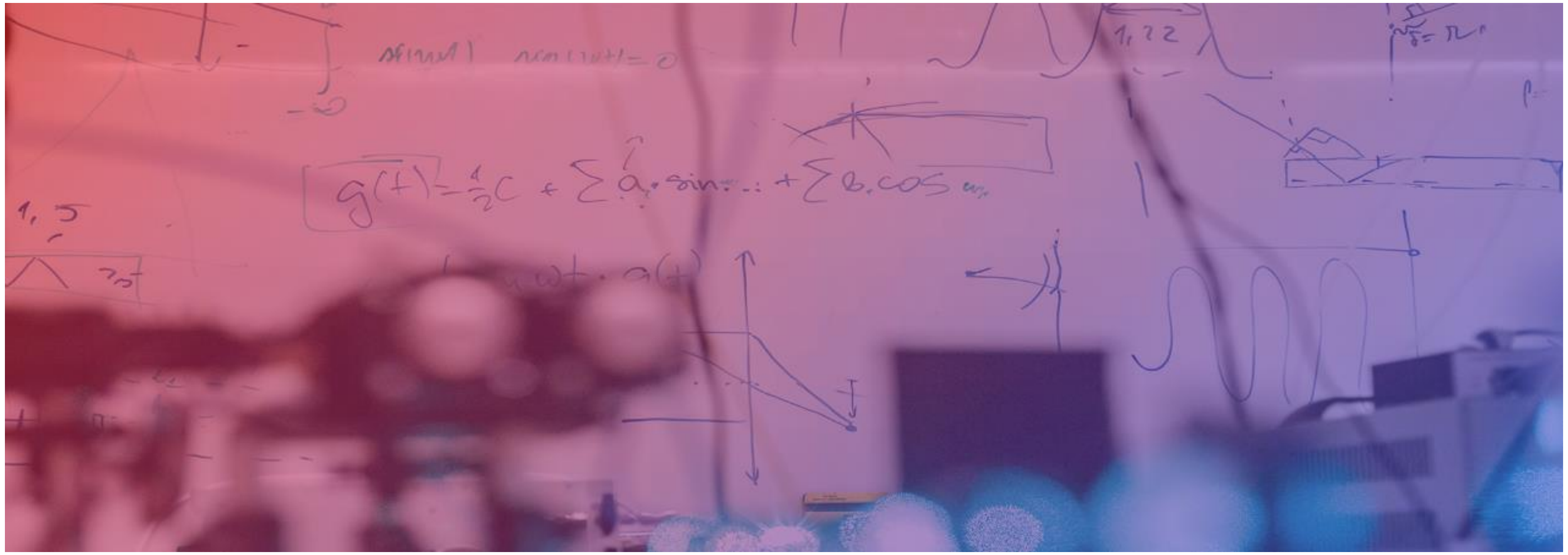
Summary

- Why is quantum different?
- Quantum algorithms
- Potential Applications
- Building a quantum computer
- What do we have so far?



Latvian Quantum Initiative
Funded by the European Union
NextGenerationEU
2027 National Development Plan

Thank you!



raqueline@gmail.com

www.quantumlatvia.lu.lv

quantumlatvia

Latvian Quantum Initiative

Funded by the European Union
NextGenerationEU

2027
National Development Plan