Quantum Computing and Qiskit

April 28, 2022 - Université de Genève

Sasha Lazarevic

LZRVC.com
www.linkedin.com/in/LZRVC

About me

Sasha Lazarevic

IBM 2003 - 2021
MSc Computer Science,
MBA

Quantum Ambassador
Qiskit Advocate

My interests

- Artificial Intelligence
- Quantum Computing
- Lecturer at EBS, ISFB
- Volunteer at Swiss Quantum Hub
- Blog: http://LZRVC.com
- Meetups :
  - https://www.meetup.com/Quantum-Computing-Switzerland-Qool-Stuff/

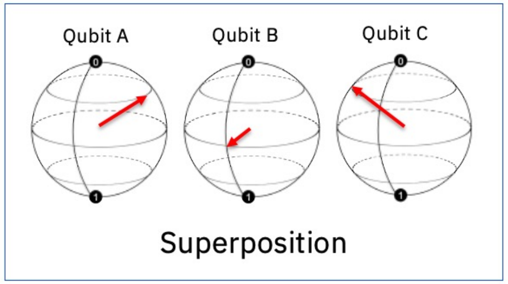
Exploiting Quantum Phenomena

Superposition

Quantum Measurement

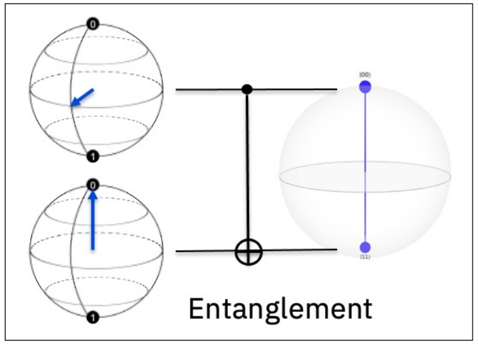
Entanglement

Interference



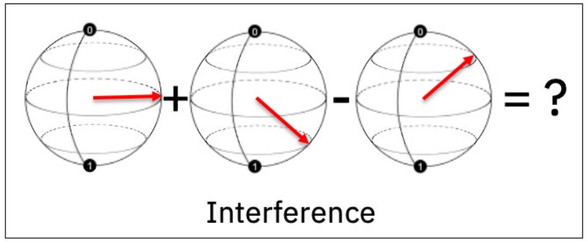
Superposition

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



Entanglement

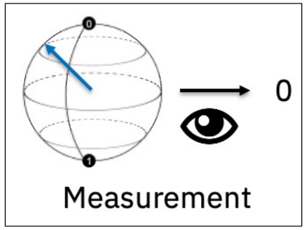
$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Interference

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$



Measurement

$$M = \begin{cases} 1\ with\ prob\ |\alpha|^2 \\ 0\ with\ prob |\beta|^2 \end{cases}$$

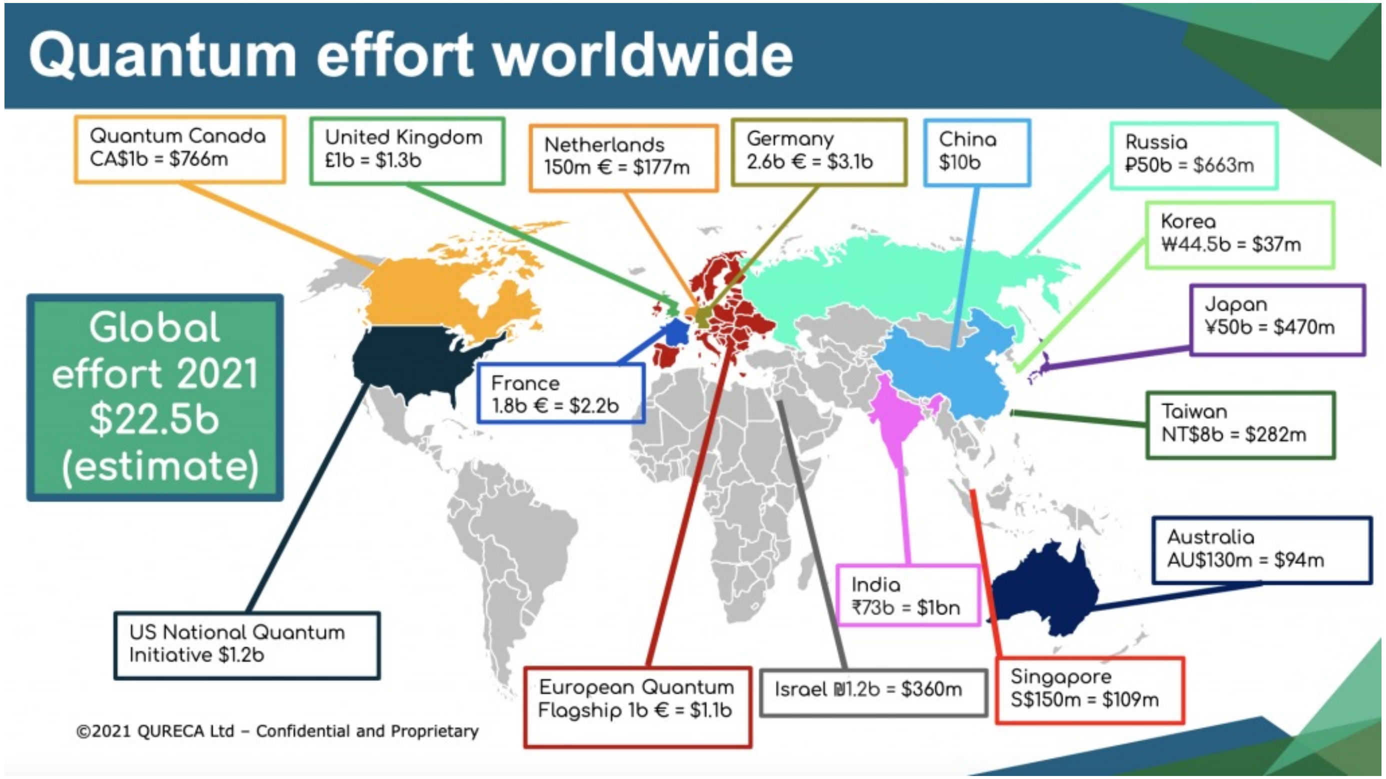
Quantum Technologies and Investments

Quantum Sensing

Quantum Communications

Quantum Annealers

Quantum Computing



Quantum Sensing

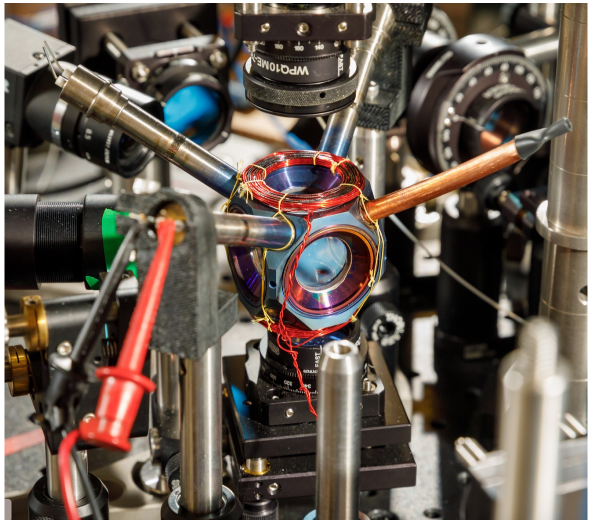
ATOMIC CLOCKS

iqClock project (https://www.iqclock.eu/) is developing mass-producible and ultra-accurate optical clock

Technologies based on:

- Cold atoms
- NV centers
- Photons
- Graphene

QUANTUM GYROSCOPES



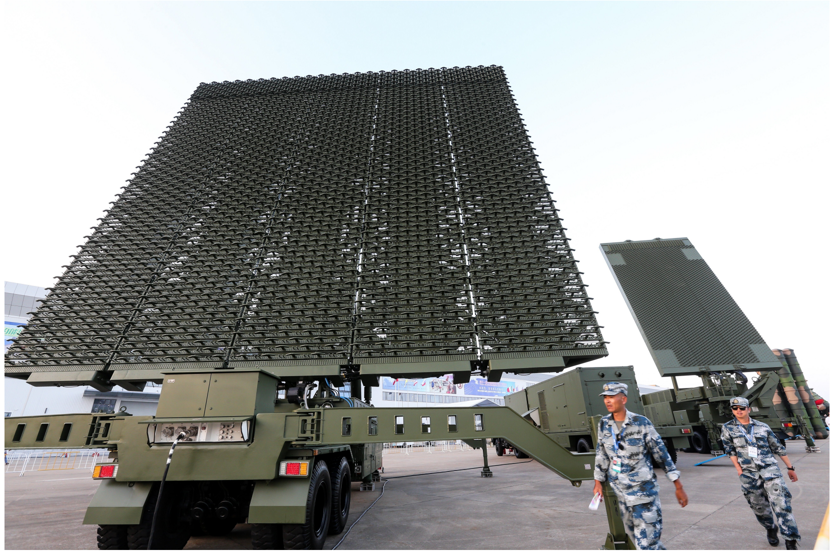
Future vehicles will use quantum sensors to measure their acceleration and rotation, so they will be able to track their own position, instead of using satellites. One of the technologies is being developed by Sandia National Labs: https://newsreleases.sandia.gov/quantum_navigation

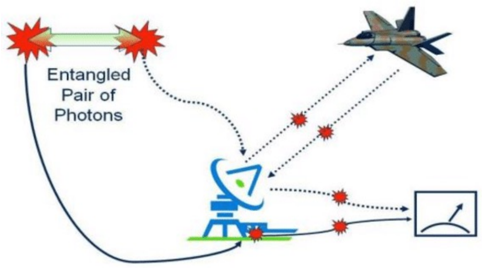
GRAVIMETERS

Identifies cavities deep underground cavities. Can be used for detecting and monitoring for vulcanic and seismic activities, oil reserves detection, in construction, search for underground oil, archeology etc

Quantum Sensing

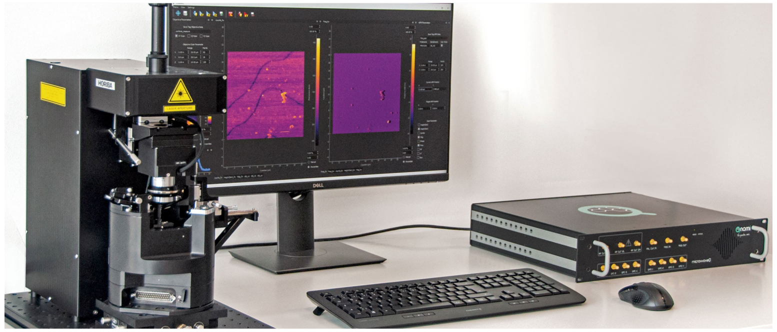
QUANTUM RADAR





Classical radars use a very strong signal which can be detected by the airplanes that can jam the signal. Quantum radars have better resolution and can use weak signal thanks to quantum entanglement

QUANTUM MICROSCOPE



Qnami (https://qnami.ch) makes nitrogen-vacancy microscope for the analysis of magnetic materials at the atomic scale

QUANTUM LIFE SCIENCE

- Quantum Scanners
- Improved MRI diagnostics
- More precise detection of cancers
- Detection of oxidative stress
- Use of quantum optically-pumped magnetometers for detecting neurodegenerative brain diseases

Quantum Communications

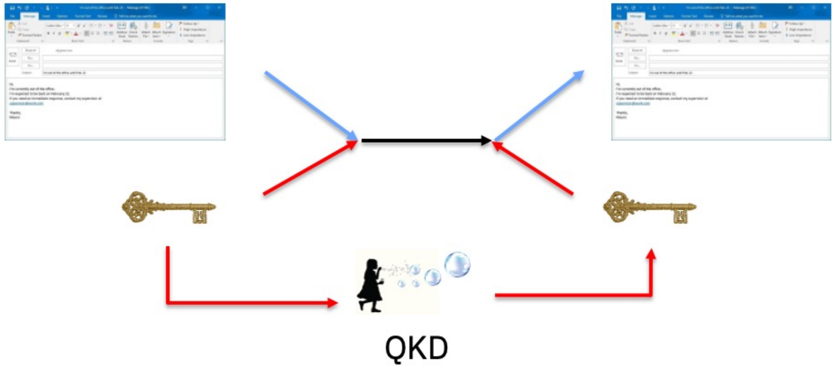
Transmission of the classical information:

- Superdense coding, quantum teleportation
- Quantum network based on remote entanglement
- Communication Security

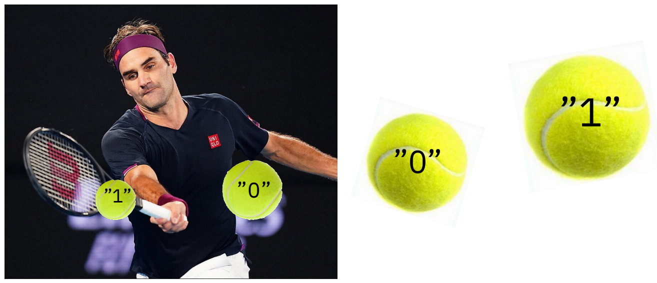
Quantum Communication Security : Quantum Key Distribution (QKD)

QKD is based on the measurement problem and no-cloning principle :

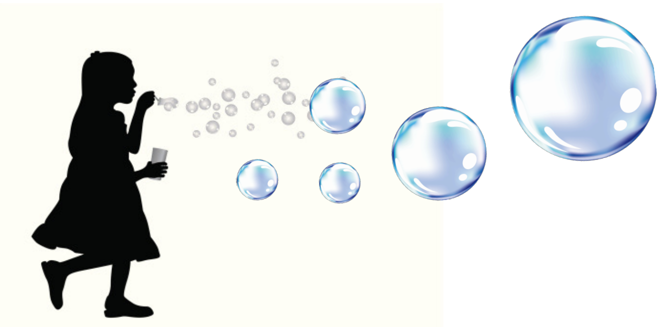
- After measurement, quantum state collapses to the basis state
- A quantum state cannot be copied



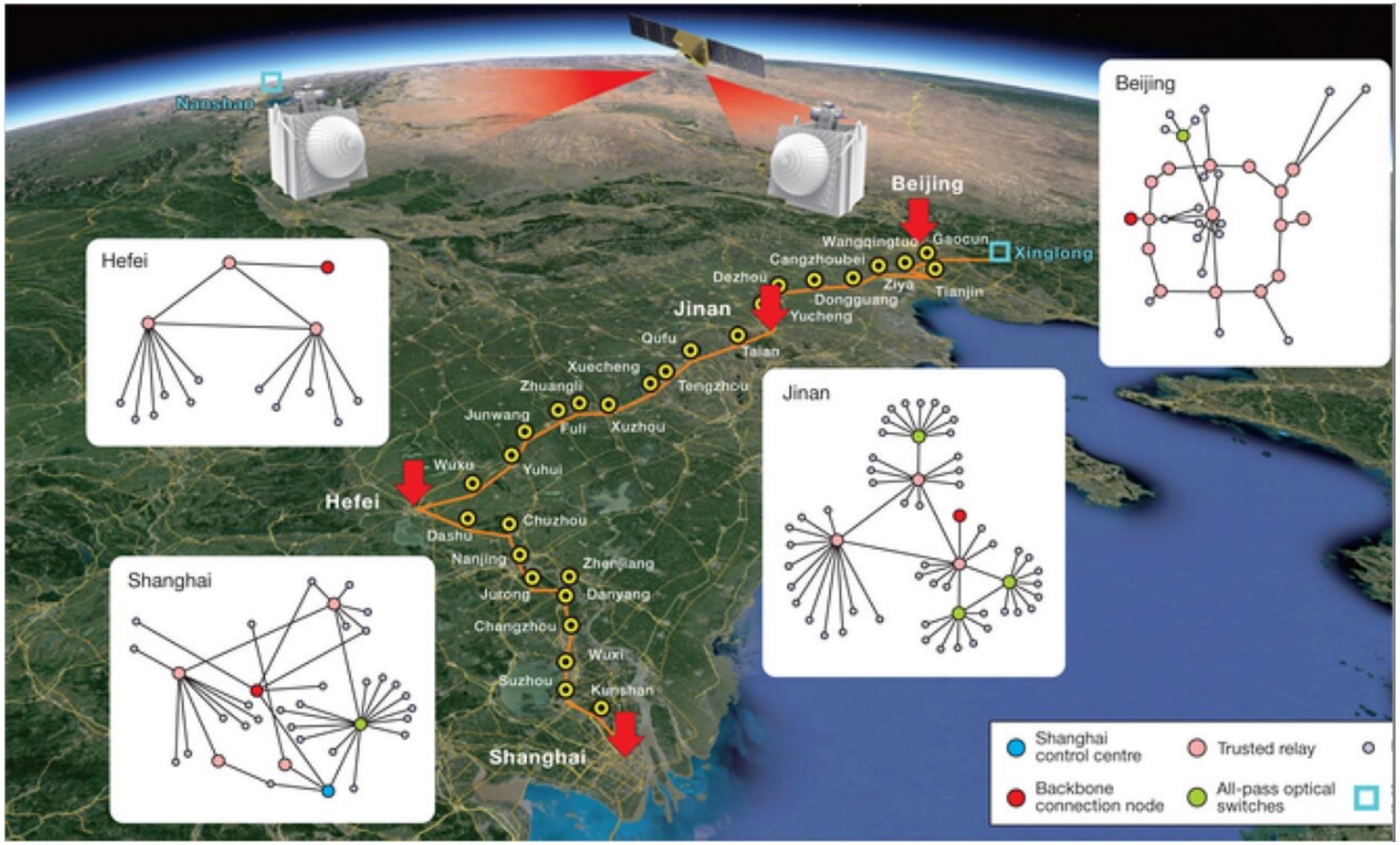
Classical communications



Quantum communications



Quantum Communications



China 2021: World’s first integrated quantum communication network over a total distance of 4’600 km

Twin-field QKD (TF-QKD) for the ground QKD to beyond 500 km

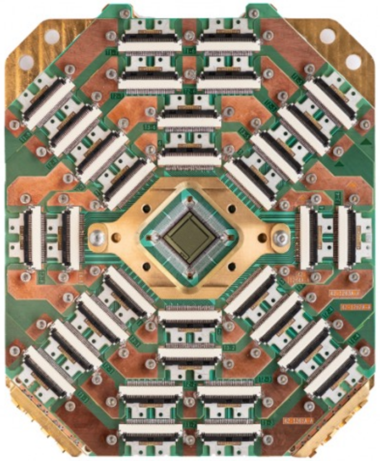
Established connectivity for more than 150 banks, power grids and government sites

Expansion of the network to Austria, Italy, Russia. Development of new satellites and ground receivers

Source: https://phys.org/news/2021-01-world-quantum-network.html

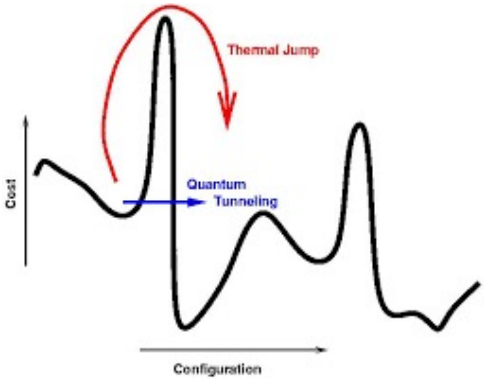
Quantum Annealers

Adiabatic Quantum Computers
D-Wave 2000Q and Advantage
superconducting flux qubits



Used for optimizations, like:

- Logistics, supply chain management
- Volkswagen traffic flow optimization
- Higgs optimization problem
- etc



With quantum annealing the system state (red) can tunnel through a changing barrier (black) and arrive at the ground state.

For classical annealing, the system relies on thermal fluctuations (temperature $T > 0$) to overcome any energy barriers.

Source: https://www.nature.com/articles/s41534-018-0060-8

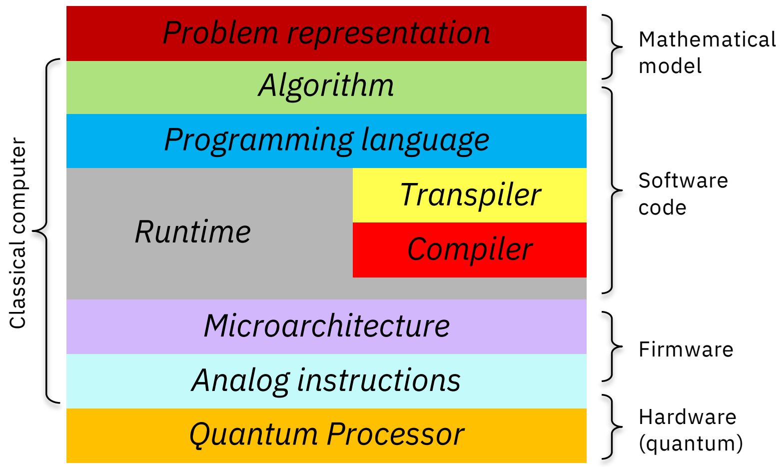
Computer specialized only for quantum annealing :

1. Set the qubits in superposition state with equal weights
2. Programmatically, but slowly (adiabatically) change the weights. This makes the system evolve, while keeping it in the ground state
3. Tunneling effect will bring it to the state of global minima

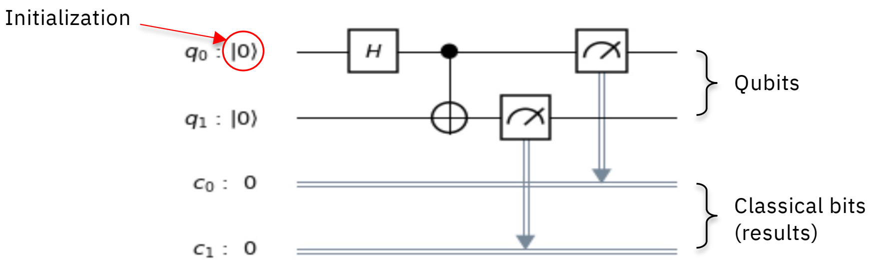
Adiabatic quantum computers don’t get excited to the higher energy state. Their state slowly evolves.

Universal Quantum Computer

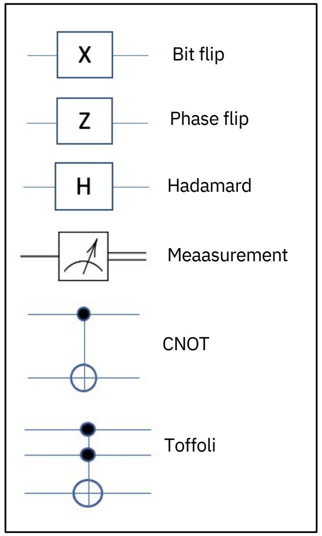
Architecture of the quantum computer


Problem representation
Algorithm
Programming language
Runtime
Transpiler
Compiler
Microarchitecture
Analog instructions
Quantum Processor
Classical computer
Mathematical model
Software code
Firmware
Hardware (quantum)

Quantum circuit



Quantum gates



Design of a quantum algorithm

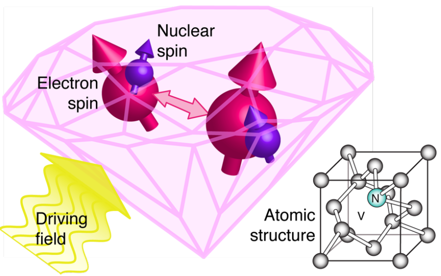
1. Exploit superposition to keep more information in quantum states

1 qubit can represent simultaneously 2 bits
2 qubits can represent 4 bits or 2^2
10 qubits can represent 2^10 bits or 128 bytes
30 qubits can represent 2^30 bits or 128 MB
40 qubits can represent 2^40 bits or 128 GB
50 qubits can represent 2^50 bits or 128 TB
…

2. Exploit entanglement to parallelize operations on these quantum states
3. Evolve the overall state to get expected results
4. Measure multiple times to get the probability distribution of these results

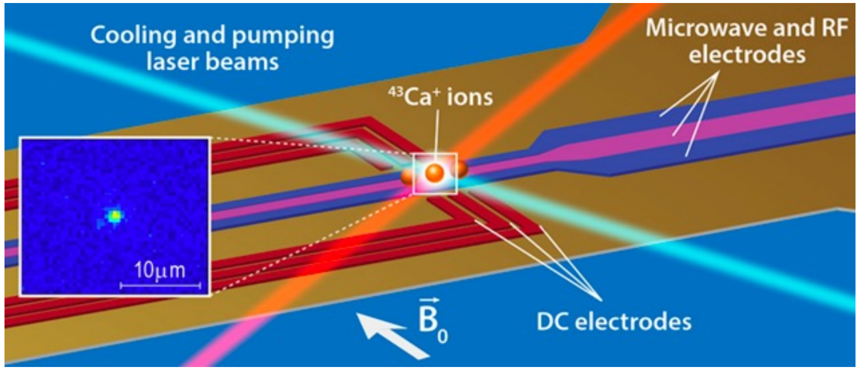
Hardware Modalities

NV Diamond Centers



Photons can be used to transfer the information and interconnect the diamonds in a network, but problem is to accurately place the defects

Ion traps (IONQ, Honeywell)

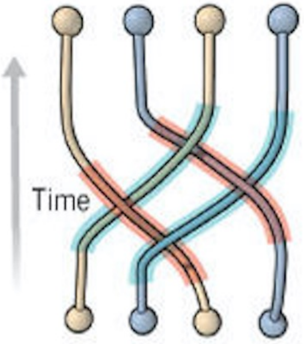


Longevity (>20m), high fidelity, but slow operations

Quantum dots (Intel)

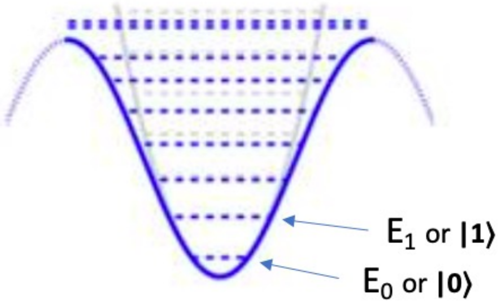
Easy to build and scale, but difficult to control, decoherence

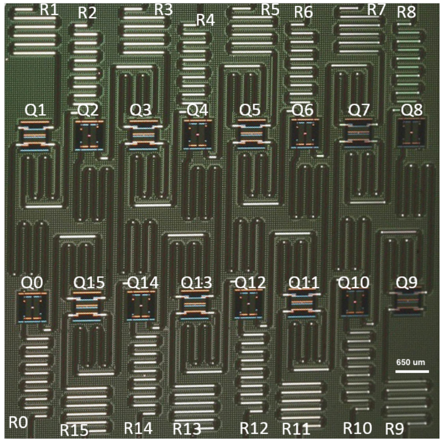
Topological (Microsoft)

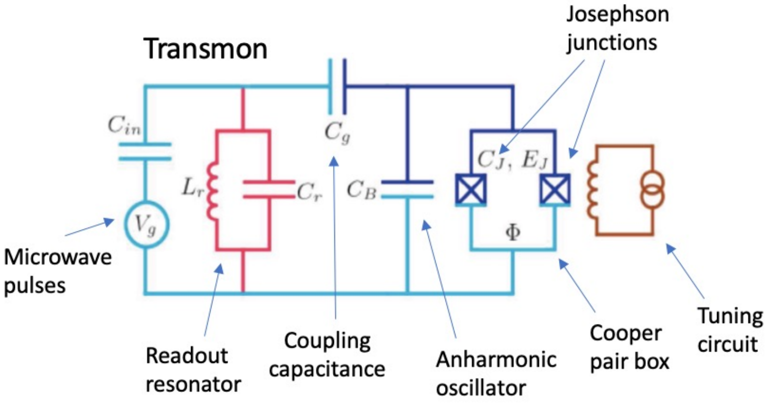


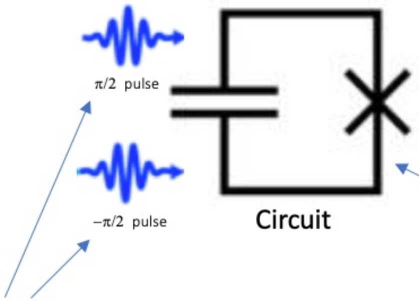
Very stable, no need for error correction, but still a research project

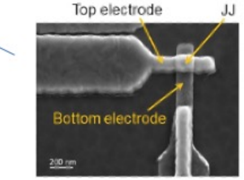
Superconducting Qubits (IBM, Google, Rigetti)











Josephson Junction
(equivalent to transistor)

Rotation gates are implemented with microwave pulses :

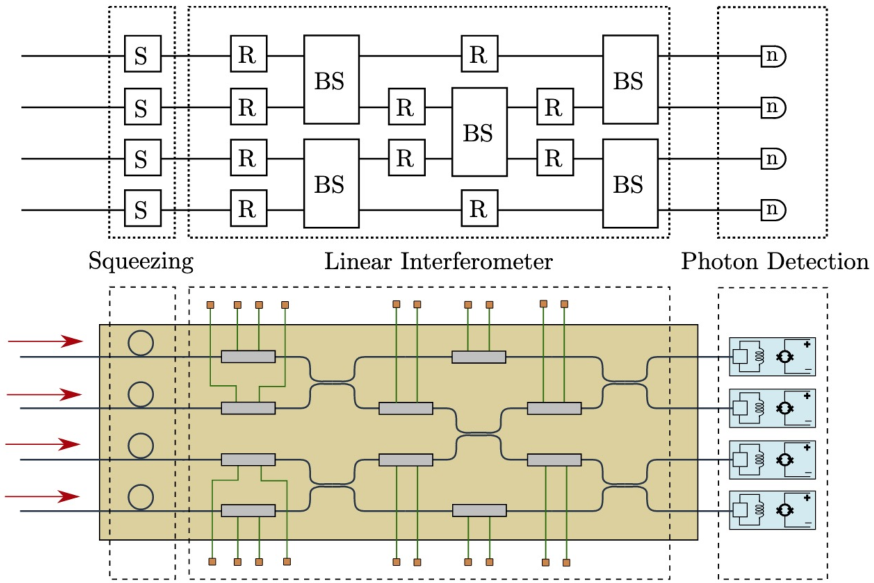
- ➢ Pulse phase 0 for X rotation
- ➢ Pulse phase π/2 for Y rotation
- ➢ Z + Y for Z rotation
- ➢ Pulse duration determines the angle

- Circuit needs to be cooled to near absolute zero
- This makes all electrons create a collective quantum state
- Energy oscillates between the capacitor and JJ anharmonically
- No resistance, only the circuit resonance
- Microwave pulses act on this resonance to change the state
- Readout is done by getting and amplifying the resonator’s signals

  Entanglement is performed by driving one qubit at the frequency of the second qubit

Photonic Computers

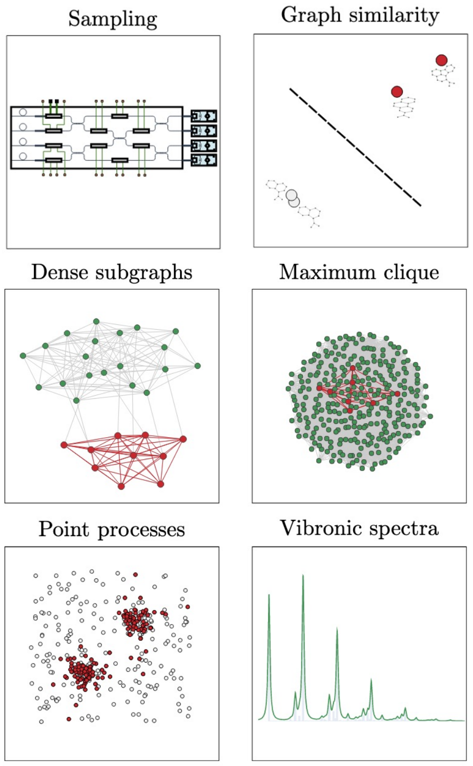
Xanadu Gaussian Boson Sampler (GBS) with 8 modes



- Laser beams are injected into the chip
- Squeezers generate squeezed vacuum state and introduce entanglement
- The squeezed light enters interferometer. The phases of the interferometer are specified from Strawberry Fields when submitting the quantum job
- The resultant Gaussian state is then measured by photon counting detectors

Source: https://strawberryfields.ai/photonics/hardware/details.html

Coding algorithms with Strawberry Fields



A graph can be naturally encoded into GBS. Many objects from networks to molecules can be modelled as graphs

Samples from a GBS device represent subgraphs. Dense subgraphs are sampled with high probability

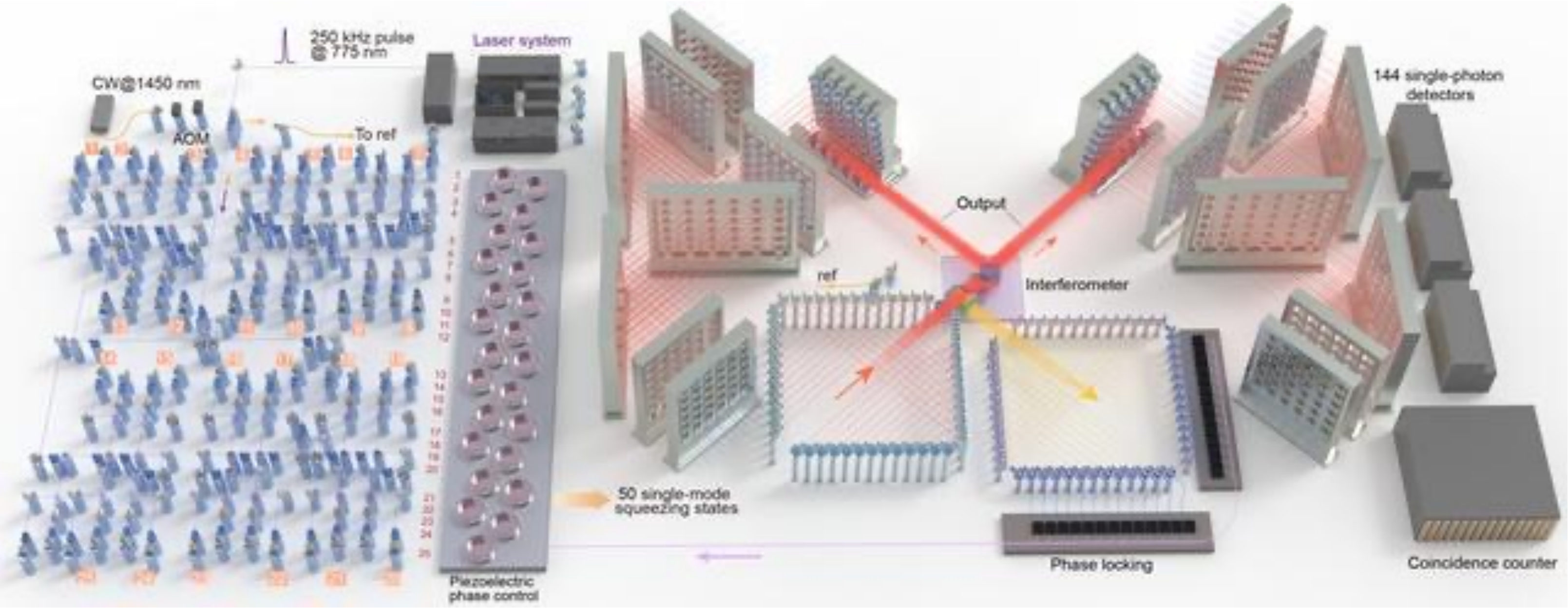
Find max-clique (hybrid algorithm): sample dense subgraphs from GBS and use them as starting points for local search

Weighted max clique algorithm can be used for the molecule docking problem. For example, determine the docking configuration between a drug and a target macromolecule (a protein in the human body)

Source: https://arxiv.org/pdf/1912.07634.pdf

Photonic Computers

Jiuzhang 2.0 GBS with 113 photons detected and 144 modes. USTC, Hefei, China in Oct 2021



“it would take the fastest supercomputer about 30 trillion years to do GBS sampling that "Jiuzhang 2.0" can do in just one millisecond”

See also: Phoqusing (https://www.phoqusing.eu/)
EU project with 3D hardware circuit and research on non-linear boson sampler

NISQ vs. fault-tolerant, large-scale quantum computer

Issues with Noisy, Intermediate-Stage Quantum Computers (NISQ) :

Superconducting qubits:

- Quantum RAM
- Quantum network
- Maximal coherence time 1ms
- Noise
- Quantum Error Correction (QEC) ratio 10’000 : 1
- Interconnectivity between qubits
- Scalability
- Cryogenics

Photonic computers :

- Source of indistinguishable photons
- Photon loss
- Configurable flexible architecture
- Quantum RAM
- Other sources of noise
- QEC

Use simulators:

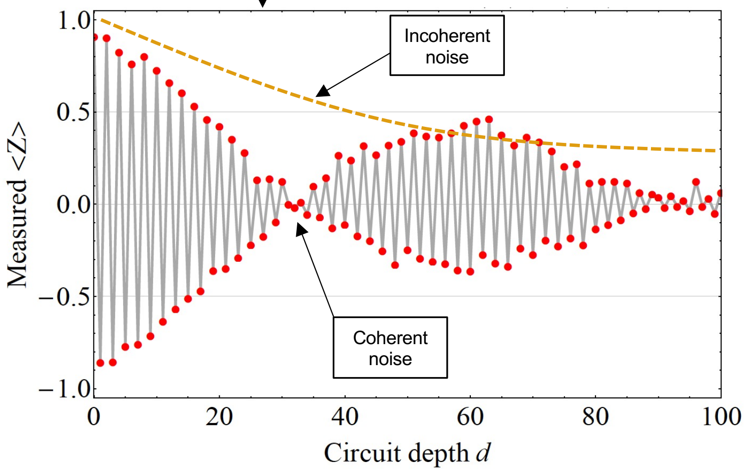
- Use your own laptop
- Servers for 30-40 qubits
- Atos Learning Machine
- Supercomputers can simulate up to 50 qubits
- Fujitsu digital annealer

Superconducting qubits operate at 12mK

Sources of noise:

- interaction with the environment,
- interactions between qubits,
- imperfect operations,
- measurement errors etc.

Intermediary solution: **error mitigation**



Source: Zlatko Minev, Qiskit Summer School 2021

Expected readiness for fault-tolerant, large-scale quantum computers, is 15 to 30 years from now !

High-Value Use Cases - Finance

Simulation

VaR / CVaR
Risk and scenario analysis
CVA and XVA
Derivative pricing

Quantum amplitude estimation (AE)

Optimization

Portfolio optimization
Optimal arbitrage opportunities
Collateral optimization
Trade settlement
Combinatorial auction

Convex optimization:
Quantum Semidefinite Programming (QSDP)

Combinatorial optimization:
QUBO -> Variational Quantum Eigensolver (VQE) / Quantum Approximate Optimization Algorithm (QAOA)

Mixed-Binary optimization:
3-ADMM-H -> QUBO with VQE/QAOA, CPLEX

Machine Learning

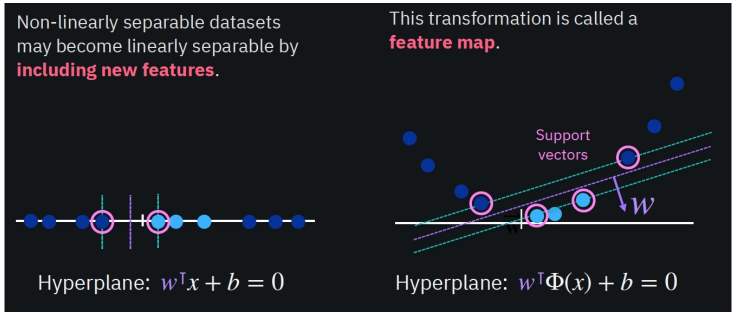
Fraud detection
Customer scoring
Forecasting
Risk estimation
Dimensionality reduction
Synthetic data generation

Quantum Kernel Estimation (QKE)
Variational Quantum Classification (VQC)
Quantum PCA (qPCA)
Quantum Circuit Born Machines (QCBM)
Quantum Boltzmann Machines (QBM)

High-Value Use Cases – Machine Learning

Quantum Kernels - SVM

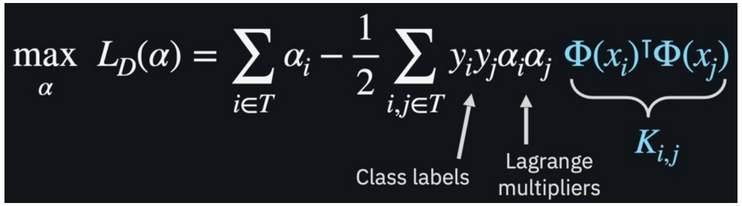
Feature maps help resolve the data non-linearity problem



Non-linearly separable datasets may become linearly separable by **including new features**.

This transformation is called a **feature map**.

Dual formulation reduces the dimensions of the search space through a function that implicitly encodes the feature map

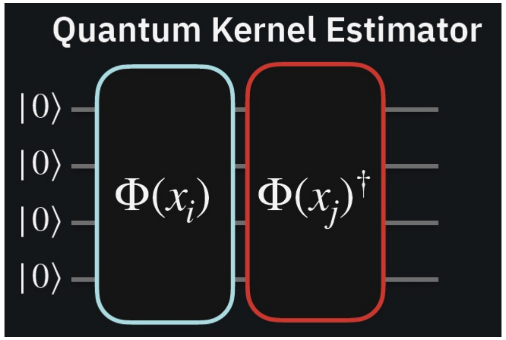


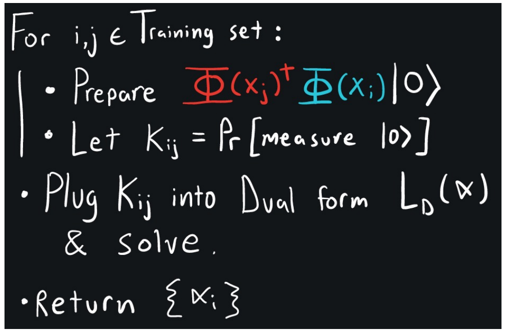
$$\max_{\alpha} L_D(\alpha) = \sum_{i\in T}\alpha_i - \frac{1}{2}\sum_{i,j\in T} y_i y_j \alpha_i \alpha_j \underbrace{\Phi(x_i)^\intercal \Phi(x_j)}_{K_{i,j}}$$

Class labels

Lagrange multipliers

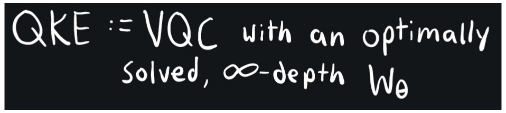
Quantum Kernel Estimator





For i,j ∈ Training set :

- Prepare $\Phi(x_j)^\dagger \Phi(x_i)|0\rangle$
- Let $K_{ij} = \Pr[\text{measure } |0\rangle]$
- Plug K_{ij} into Dual form $L_D(\alpha)$ & solve.
- Return $\{\alpha_i\}$



QKE := VQC with an optimally solved, ∞-depth W_θ

But to ensure quantum speedup, the quantum kernel function $\Phi(x)$ has to be hard to estimate clasically.

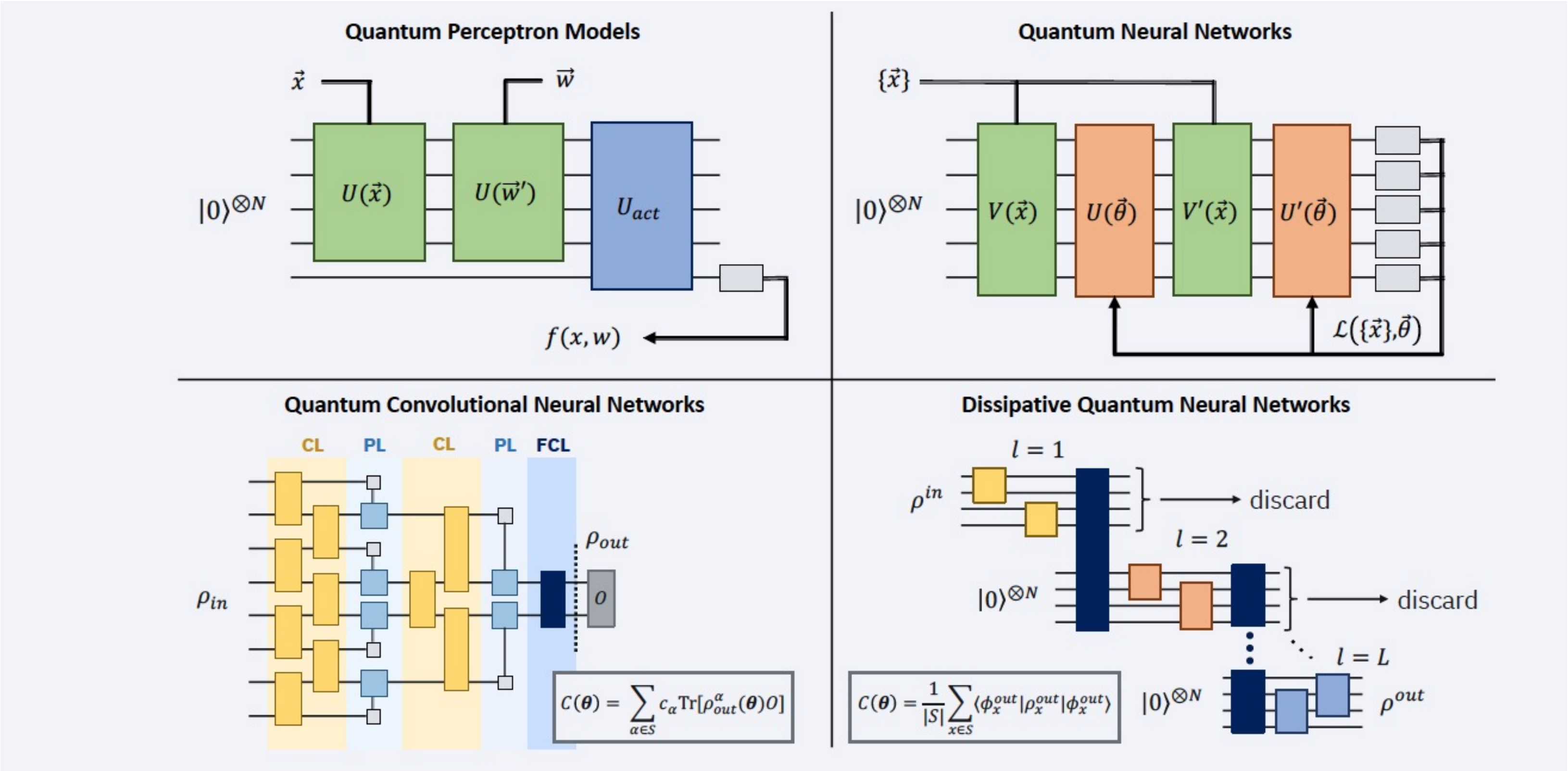
Idea: Design quantum kernels to exploit the group structure in data.

Example is **DLOG kernel**

Sources:
Global Qiskit Summer School 2021
https://arxiv.org/pdf/2010.02174.pdf

High-Value Use Cases – Machine Learning

Quantum Neural Networks

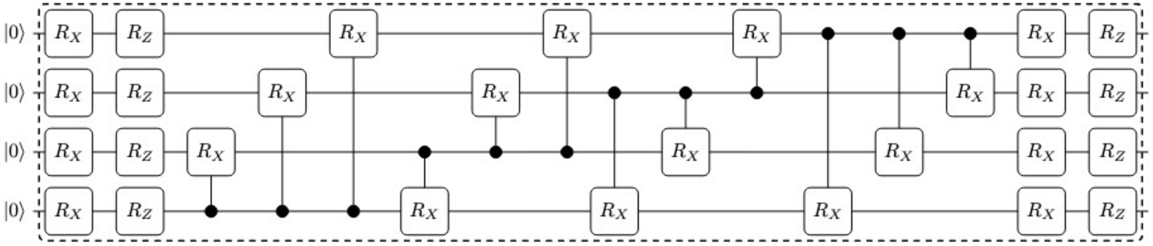


Quantum Machine Learning – Training Process

Training procedure :

1. Data Encoding
   - Angle
   - Amplitude
   - High-order
2. Variational Circuit
   - Expressive power
3. Measurements (readouts)
4. Cost Function
5. Gradient Descent
6. Update parameters
7. Run again until convergence

Beware of the barren plateau !

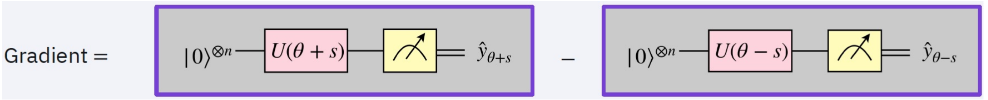


- Higher entangling capability means being better able to capture non-trivial correlations in the input data
- Expressivity increases with stacking up several layers

Labels extraction :

- based on parity or
- measuring only the first qubit

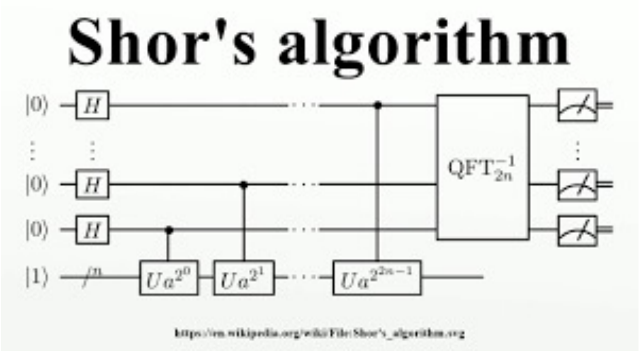
- Parameter shift rule
- Natural gradient



Other Use Cases - Security

Key Insights

- Shor’s algorithm can break RSA encryption
- For RSA 2048 it requires around 5’000 qubits
- But these qubits need to be of high quality
- Current quantum computers can’t run factoring of even the number like 35 (7 x 5). The largest instance factored was 21 (7 x 3)
- It is estimated that it will take 30 years to get quantum computers capable of this task
- Impacted are : internet, banks, military, bitcoin, car manufacturers, avionics …
- Future generation of quantum-safe encryption standards is being prepared (MNIST, ITU standards)
- Huge work expected to migrate RSA and ECC to the new solutions
- Symmetric encryption schemas like AES 256 or AES 512 not impacted



https://en.wikipedia.org/wiki/File:Shor's_algorithm.svg

15 = 3 x 5

38647884621009387621432325631 = ? x ?

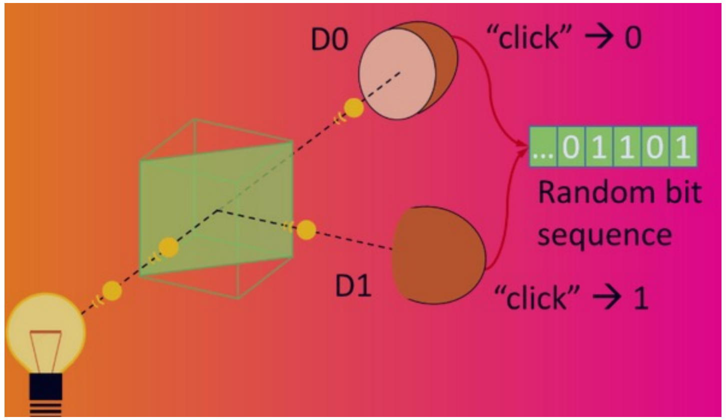
~~RSA~~

Other Use Cases - Security

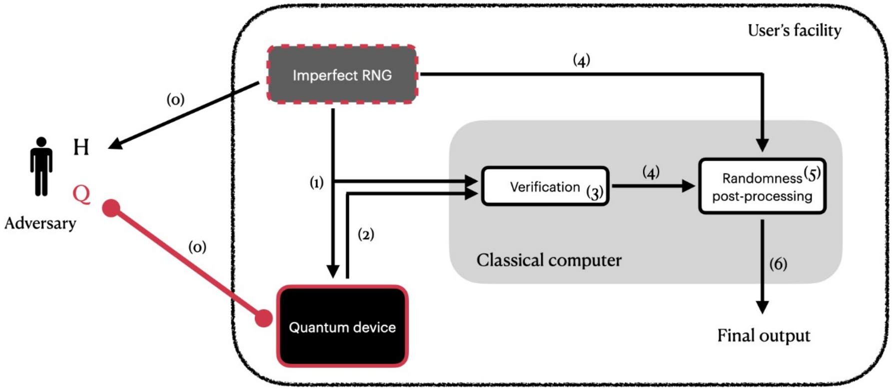
Quantum Random Number Generators (QRNG) produce random numbers from the quantum superposition and measurement

Can be implemented based on:

- Software relying on quantum processors: IronBridge by Cambridge Quantum
- Hardware chips or cards with software for the control of randomness : scaling, extraction, storing etc

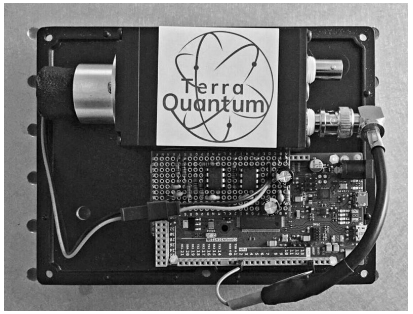


Source: https://qt.eu/discover-quantum/underlying-principles/qrng/



Source: https://arxiv.org/pdf/2009.06551.pdf

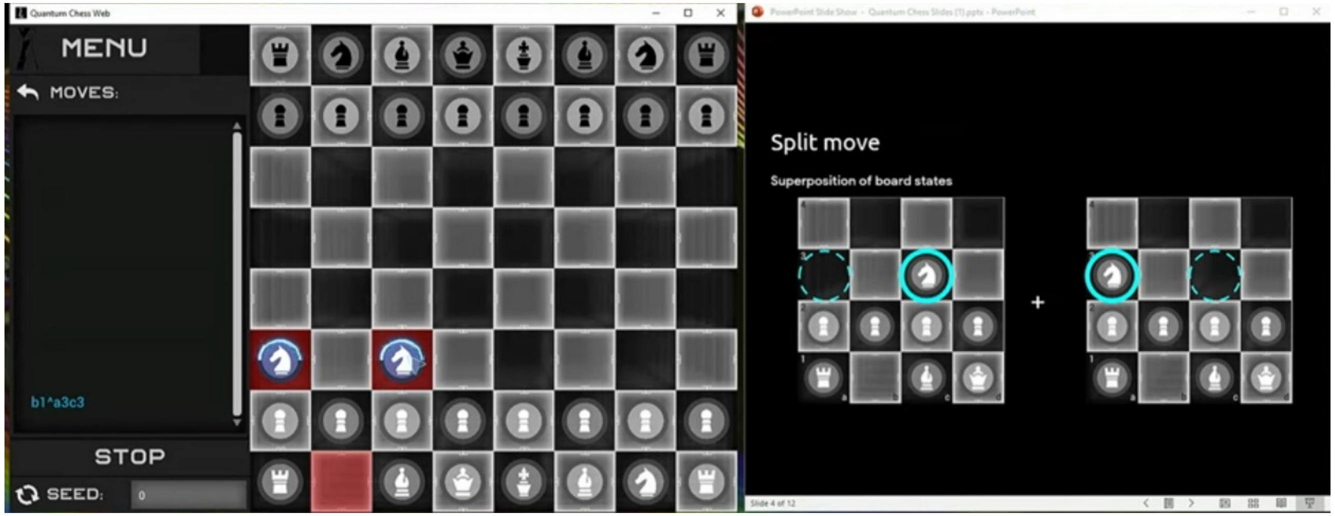
ID Quantique



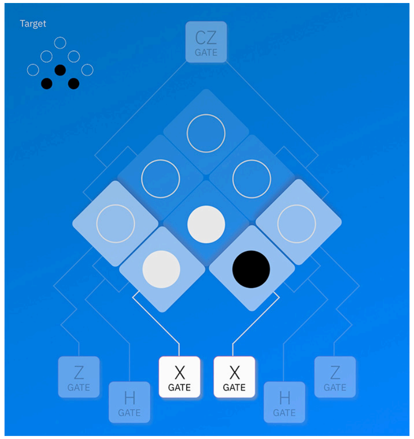
https://qm-ware.com

Other Use Cases – Quantum Games

Quantum Chess



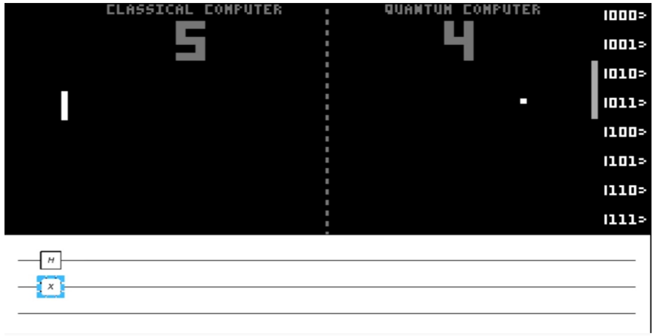
Source: https://quantumchess.net



Hello
Quantum

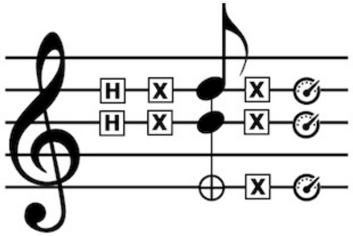
On Google Play Store, Apple Store

QPong

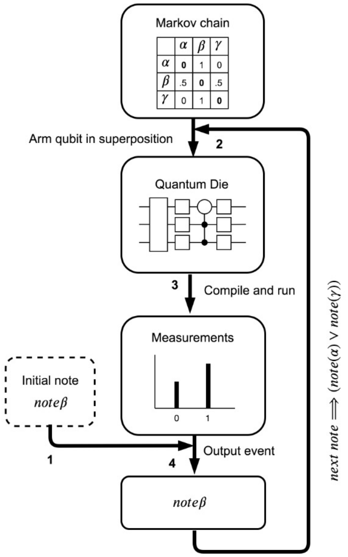


Source: https://github.com/JavaFXpert/quantum-pong

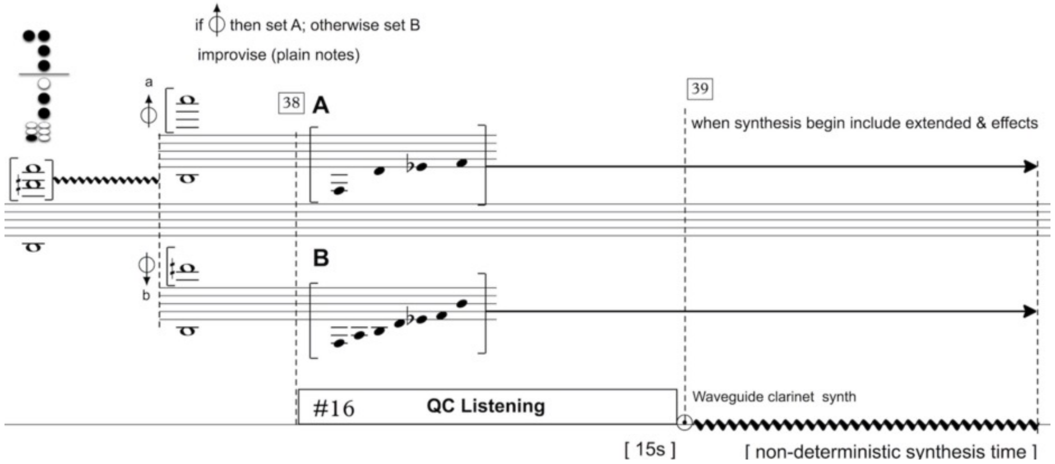
Other Use Cases – Quantum Arts (Music)

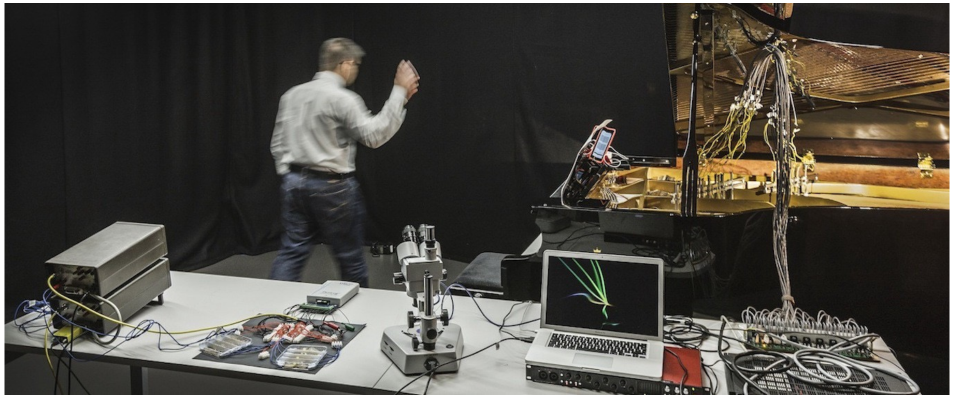


Musical Quantum Walk



Source: https://arxiv.org/pdf/2110.12408.pdf





Eduardo Reck Miranda : https://twitter.com/bio_computer

How does this impact You ?

In 3-5 years:
- First practical use cases with quantum advantage
- Quantum network
- Narrow selection of successful hardware modalities
- But also, shortage of access to real quantum computers

In 10 years:
- New quantum algorithms which shorten the time to major breakthroughs
- Migrations of encryption schemes to quantum-safe protocols
- Quantum memory
- Error correction mechanisms

In 20 years:
- Fault tolerant quantum computer able to run deep circuits
- Implementation of high-value use cases

How can you learn Quantum computing

Books :

- Quantum Computation and Quantum Information by M. Nielson, I.Chuang
- Qiskit Textbook (https://qiskit.org/textbook) by IBM
- Machine Learning with Quantum Computers by Maria Schuld
- Introduction to Quantum Information Science by Vlatko Vedral
- Quantum Computing for Computer Scientists by Noson Yanofski
- Quantum algorithms for data analysis (https://quantumalgorithms.org)

Courses :

- CaltechX, DelftX (2018) Quantum Cryptography (edX, online)
- Keio (2018) Understanding Quantum Computers (futurelearn.com, online)
- IBM Qiskit Summer Schools (in July, online)
- TUDelft (2021) The Hardware of a Quantum Computer (edX, online)

Private courses for your organization (contact me)

Useful Links

EU Qualification Profiles for Quantum Technologies:
https://qt.eu/app/uploads/2022/01/QualificationProfilesQuantumTechnology_Beta_Jan2022.pdf

EU Quantum Technologies Competence Framework:
https://qt.eu/app/uploads/2021/09/CompetenceFrameworkQuantumTechnologiesV1.pdf

Qiskit Textbook:
https://qiskit.org/textbook/preface.html

High-level structure of Qiskit:
https://qiskit.org/documentation/stable/0.24/the_elements.html

IBM Quantum circuit composer:
https://quantum-computing.ibm.com/composer/files/new

Your next steps

Join :

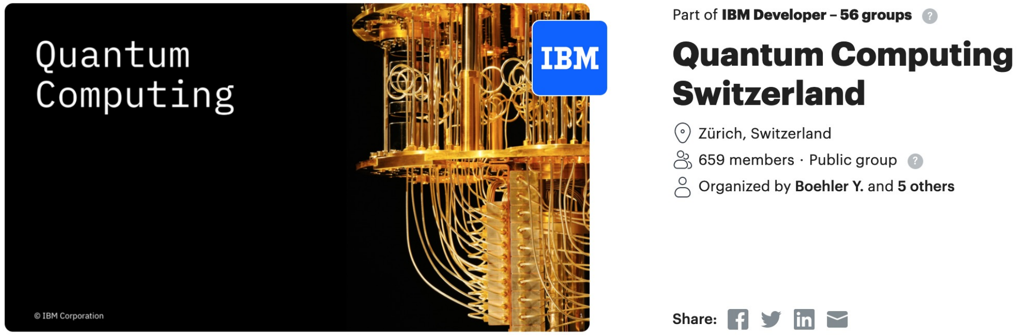
SwissQuantumHub

https://www.swissquantumhub.com/

Quantum Computing Switzerland

Listed group

https://www.linkedin.com/groups/9094236



Part of **IBM Developer – 56 groups**

Quantum Computing Switzerland

Zürich, Switzerland

659 members · Public group

Organized by **Boehler Y.** and **5 others**

Share:

https://www.meetup.com/Quantum-Computing-Switzerland-Qool-Stuff/

Qiskit

https://qiskit.org/advocates/

Thank you!

Sasha.Lazarevic@gmail.com
SashaL@swissquantumhub.com
www.linkedin.com/in/LZRVC

LZRVC
.com
tech think tank