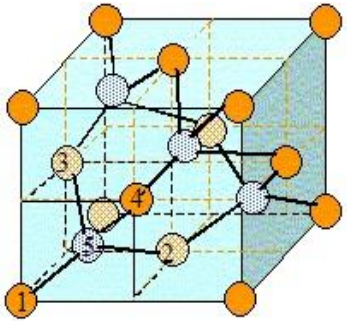
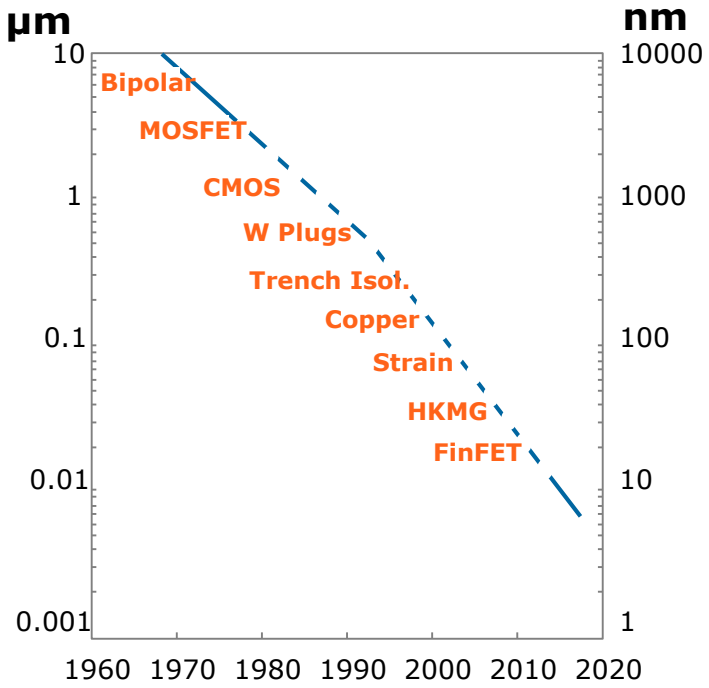
Business club – 15 Janvier 2020
Le programme Atos Quantum

Philippe Duluc,
Atos CTO Big Data & Security
Distinguished Expert – Atos Scientific Community

Atos

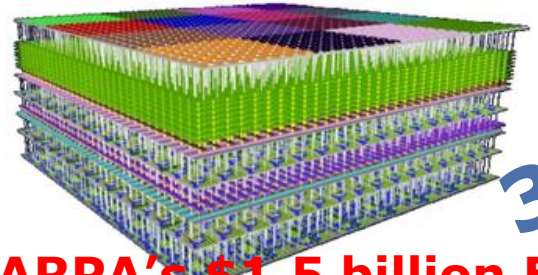
The computing disruption





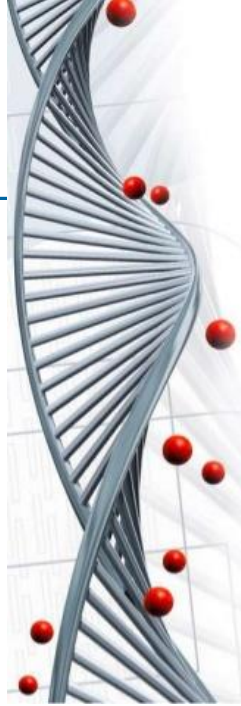
- Moore's law declining: 0,3 nm between 2 atoms in Silicon crystal, chip fabrication process < 10 nm
- obligation for Atos to find new directions in order to provide accelerations required by customers

Alternatives to CPU?



3DCPU?

DARPA's $1.5 billion Electronics Resurgence Initiative (ERI): the Three Dimensional Monolithic System-on-a-Chip (3DSoC) program



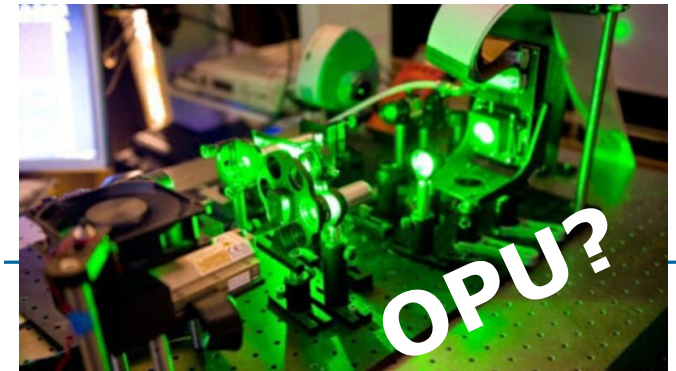
Why Bio Computing ??

- Moore's Law states that silicon microprocessor complexity will double in every 18 months.
- One day this will no longer hold true when miniaturization limits are reached.
- Solving complex problems which today's supercomputers are unable to perform in stipulated period of time.
- Require a Successor to Silicon

BPU?

ABDULLAH FARHAD

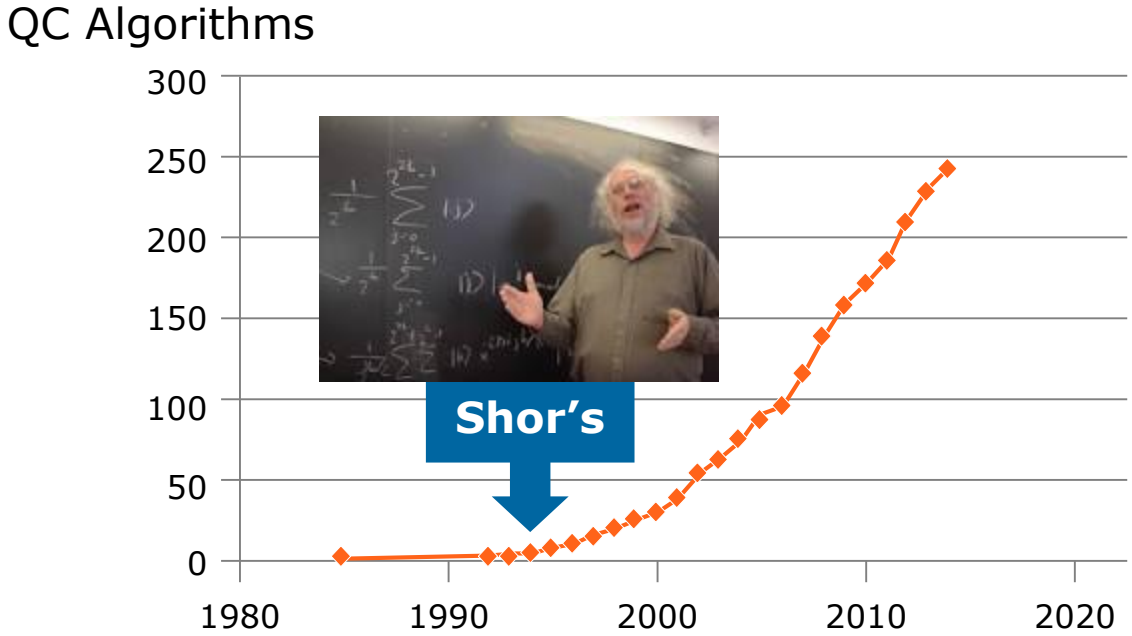
LightOn



OPU?

Atos

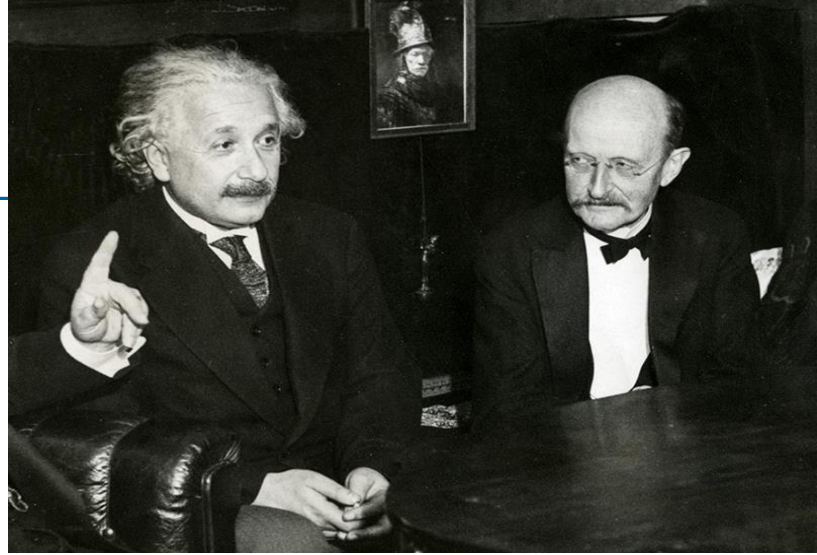
Algorithmic innovation has launched the Quantum Big Race



math.nist.gov/quantum/zoo

Atos

Quantum revolutions



- Max Planck, 1900:
  - « quantas » father
  - Nobel prize 1918 for discovery of energy quantas
- Albert Einstein, 1905:
  - photoelectric effect : real nature of light (photons)
  - duality waves/corpuscles : Nobel prize 1921
- First Quantum revolution, 1930- :
  - quantum chemistry, electronics, lasers, transistors, semiconductor industry, nuclear magnetic resonance, optical fibers, etc.
- Second Quantum revolution, 1950- :
  - quantum information, quantum cryptography, quantum computing, quantum networks, etc.
  - taking advantage of two disruptive physical properties :
    - **superposition** : a qubit (equivalent of bit in quantum world) has 2 states, and keeps its two possible values 0 and 1, superposed, until the end of the computing cycle
    - **entanglement** : when n qubits are entangled, they form a single quantum object having 2^n states, and keeping its 2^n possible values superposed until the end of the computing cycle

Quantum information fundamentals

Superposition & entanglement

1 qubit: superposition of 2 states |0> and |1>

n qubits entangled: superposition of 2^n states |0…00>, |0..01>, ……, |1…10> and |1…11>

Quantum acceleration

operations on qubits are computed on all 2^n states, superposed and entangled, **at the same time**

Max speedup of qubits vs classical bits is exponential (nx2^n vs nx1)

Only one state as the result of measurement : quantum algorithms can reach speed-up on hard problems (factorization, sorting, matrix inversion)

60 entangled qubits are more powerful than a exaflopic computer processing one billion of billion Operation per second

The cybersecurity disruption

TODAY/PAST (pre-quantum)

- classical factorization record for **RSA768** in 2010. Two years of computing on several hundreds machines to factorize this :

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

=

334780716989568987860441698482126908177047949837137685689124313889828837938780022876147116525317430877378144679994 89

×

367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17

- comp[**RSA1024**] = comp[**RSA768**] * 10^{37}

This exponential complexity is the keystone of RSA crypto algorithm (and almost all asymmetric algos)

TOMORROW (post-quantum)

- Shor Algorithm: polynomial time
- RSA-768 : almost instantaneous by using a quantum computer with several thousands logical Qubits
- comp[**RSA1024**] = comp[**RSA768**] * 2,4

Critical risk (very high impact, low prob.) for IT security everywhere

Atos

Atos Quantum : a long-term strategic R&D investment of disruptive innovation, set up in 2016

- Atos worldwide leader in supercomputing and European leader in cybersecurity

Quantum Computing will affect sooner and later Atos supercomputing customers and cybersecurity customers

- **Business rationale**
  - **strategic move to keep business leading positions**
  - **aiming mid-term RoI**
  - **in close touch with customers**

Atos

Atos Quantum Program

Atos QLM
Atos Quantum Learning Machine

Focus on quantum software, agnostic in quantum hardware: in 2017 commercialization of **Atos QLM** which is an appliance making easy to develop quantum algorithms (programing, optimising and testing via emulation up to 41 qubits); in 2019 introduction of **myQLM** software and creation of **QLM user-group**

Atos Quantum Accelerator

R&D program with hardware partners: to deliver in 2023 a **NISQ accelerator** (50 to 100 physical qubits) for hybrid supercomputing and driven by **Atos QLM**

Atos Quantum-safe security

Aligned with NIST call for post-quantum standards: preparing the cryptographies and hardware security modules, resistant to quantum attacks

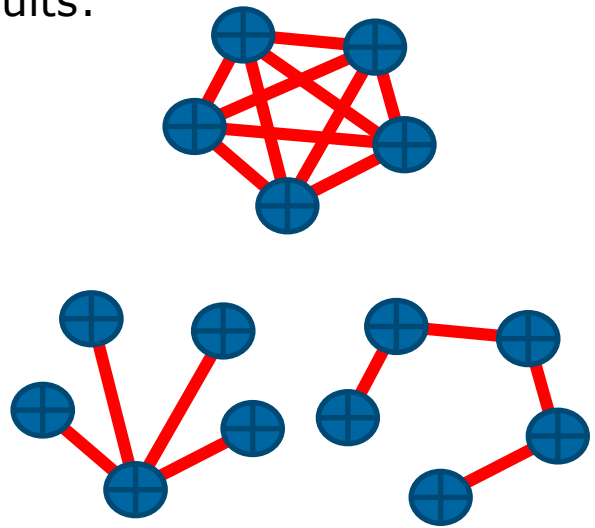
Atos

Atos QLM customers

- commercial success in a new market
- huge interest immediately after announcement in July 2017
  - for education (universities)
  - for research (research centers, university labs)
  - for HPC ecosystems (post Moore's law)
  - for industry (first contracts)

From linear simulation to realistic simulation

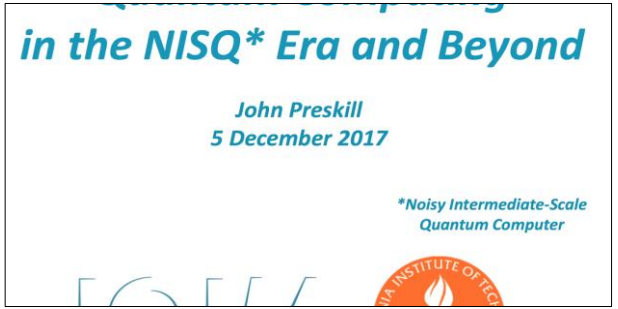
- leading hardware technologies for qubits-based circuits:
  - trapped ions qubits
  - superconducting qubits
  - semiconducting qubits
- performances of algorithms are **HW dependent**:
  1. qubit topology, connectivity, gate limitation
  2. stability, quantum noise (decoherence)
  3. speed, shallowness, idling time
- **Atos QLM** integrates hardware constraints
  - powerful compiler and optimizers
  - testing more realistic (integrating noise models and topology)
  - true performance over present and future accelerators



Atos

Atos priorities

Priority to **applications and algorithms** with quantum advantages



1. We have entered the NISQ era
   - quantum advantage within 3-5 years
   - **Atos Quantum Accelerator** within 3-5 years

2. Develop and optimize NISQ algorithms and applications with **Atos QLM**
   - focus on shallow circuits for hybrid algorithms: chemistry/VQE, machine learning/QAOA
   - focus on DQS: quantum chemistry, material science, nuclear physics
   - POCs already engaged with industrial customers

Optimizing fidelity with QLM