Quantum Computation

Lake Garda, September 2018

José Ignacio LATORRE
Univ. Barcelona / National Univ. Singapore
Quantic@BSC-UB

Hillary Clinton wants “Manhattan-like project” to break encryption

US should be able to bypass encryption—but only for terrorists, candidate says.

by **Jon Brodkin** - Dec 21, 2015 5:15pm CET

Enlarge / Hillary Clinton.

Clinton campaign.

Presidential candidate Hillary Clinton has called for a "Manhattan-like project" to help law enforcement break into encrypted communications. This is in reference to the Manhattan Project, the top-secret concentrated research effort which resulted in the US developing nuclear weapons during World War II.

At Saturday's Democratic debate (transcript here), moderator Martha Raddatz asked Clinton about Apple CEO Tim Cook's statements that any effort to break encryption would harm law-abiding citizens.

2B€ Mission

+HPC
!!!

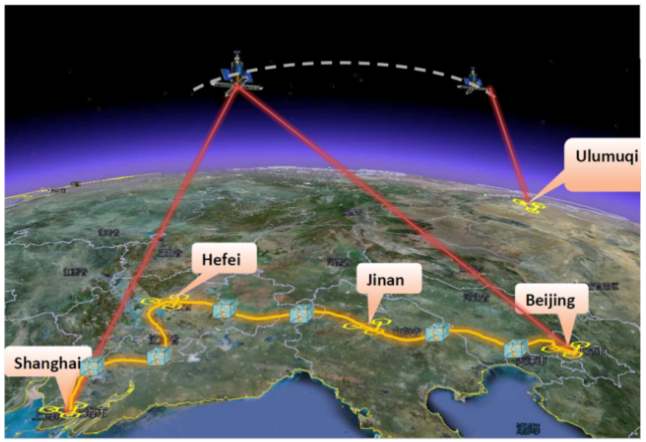
1B€ Flagship

China

NATIONAL LABORATORY FOR QUANTUM INFORMATION SCIENCES

The $10 billion National Laboratory for Quantum Information Sciences in Hefei will be the center of China's attempt to take the global lead in quantum computing and sensing.

CNTV



48 trusted nodes

Micius satellite
Tibet, 1200 km apart
Austria-China (9/2017)

Wolfsburg/Hanover, 20 March 2017

Research project successful: Volkswagen IT experts use quantum computing for traffic flow optimization

- **CeBIT 2017: Volkswagen announces cooperation with leading quantum computing company D-Wave Systems**
- **First research project successful: travel times of 10,000 taxis in mega-metropolis of Beijing significantly reduced**

Dr. Christian Seidel, Senior Data Scientist from Volkswagen Group IT's Data Lab in Munich, Robert „Bo" Ewald, President D-Wave International, Dr. Martin Hofmann, CIO of Volkswagen Group, Dr. Fl...

The Volkswagen Group is the world's first automaker to intensively test the use of quantum computers. Volkswagen is cooperating with leading quantum computing company specialist D-Wave Systems. At CeBIT 2017, the two companies today announced their cooperation. In a first research project, IT experts from Volkswagen have already successfully developed and tested a traffic flow optimization algorithm on a D-Wave quantum computer.

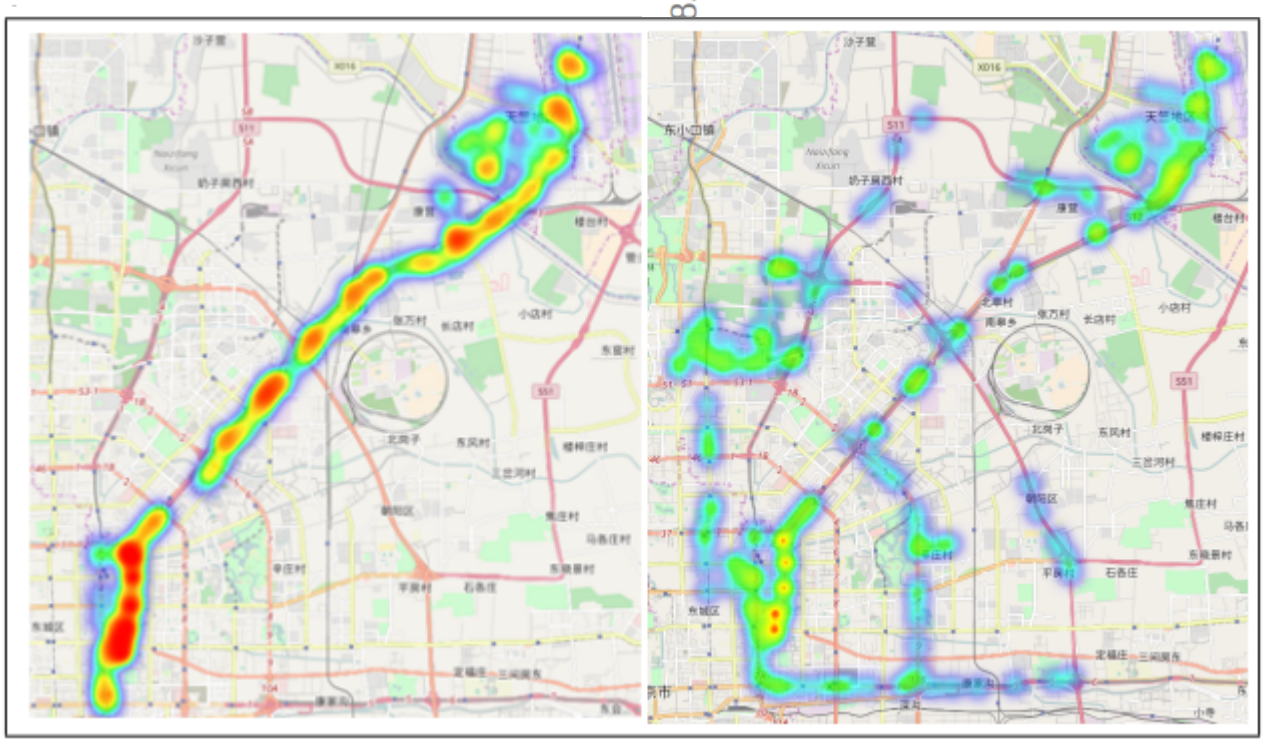
Traffic flow optimization using a quantum annealer

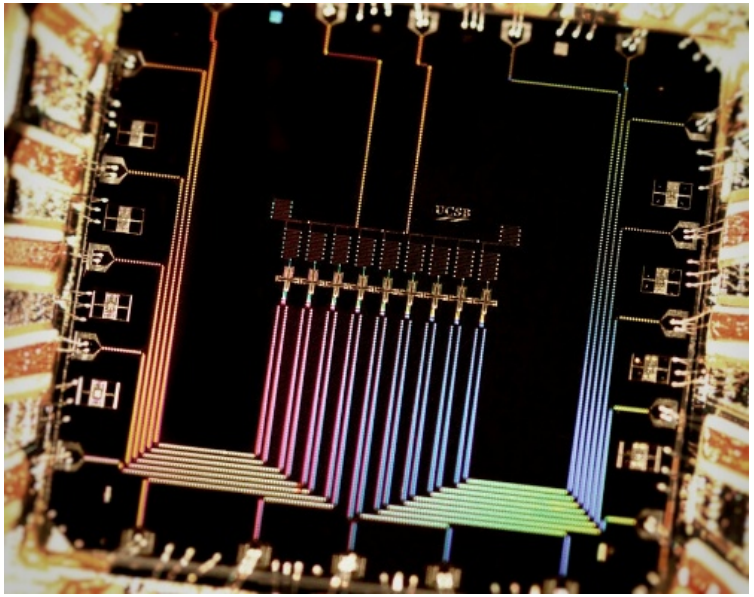
Florian Neukart*[1], David Von Dollen[1], Gabriele Compostella[2], Christian Seidel[2], Sheir Yarkoni[3], and Bob Parney[3]

[1]Volkswagen Group of America, San Francisco, USA
[2]Volkswagen Data:Lab, Munich, Germany
[3]D-Wave Systems, Inc., Burnaby, Canada

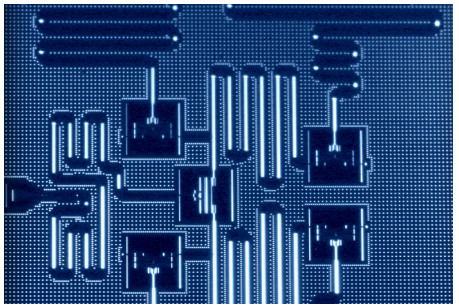
Abstract

Quantum annealing algorithms belong to the class of meta-heuristic tools, applicable for solving binary optimization problems. Hardware implementations of quantum annealing, such as the quantum processing units (QPUs) produced by D-Wave Systems, have been subject to multiple analyses in research, with the aim of characterizing the technology's usefulness for optimization and sampling tasks. In this paper, we present a real-world application that uses quantum technologies. Specifically, we show how to map certain parts of a real-world traffic flow optimization problem to be suitable for quantum annealing. We show that time-critical optimization tasks, such as continuous redistribution of position data for cars in dense road networks, are suitable candidates for quantum computing. Due to the limited size and connectivity of current-generation D-Wave QPUs, we use a hybrid quantum and classical approach to solve the traffic flow problem.

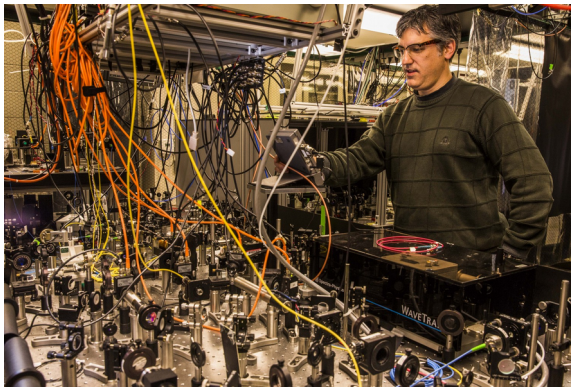




Martinis Google
72 qubits (24 operative)



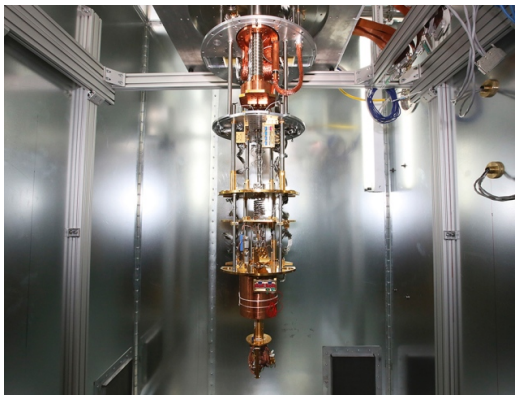
IBM cloud computer
5, 16, 20 qubits



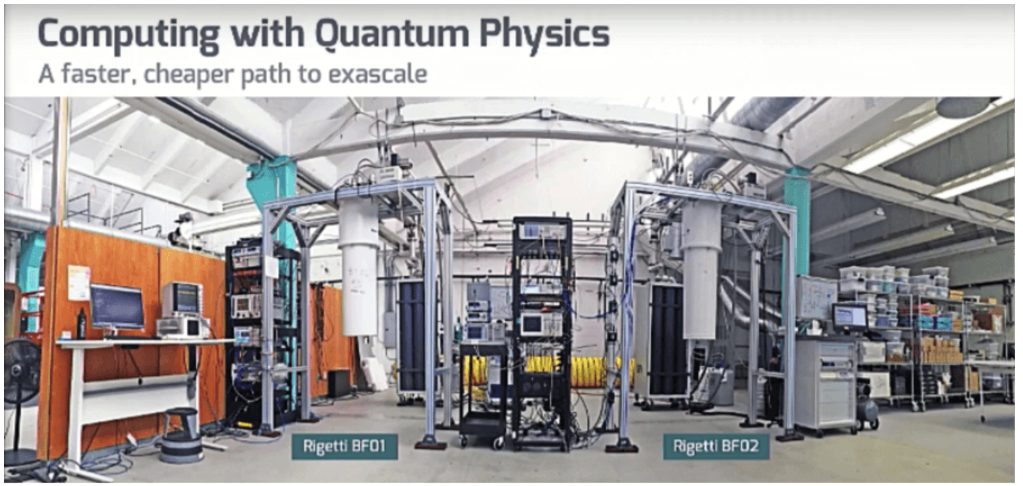
IonQ
9 qubits

STATION Q

Microsoft
0 qubits



DWAVE2
2048 non coherent qubits



Rigetti
16 qubits, 128 (coming)

Qilimanjaro: 1 qutrit

QM = Information

QM ➡ Information

Von Neumann & Copenhagen interpretation

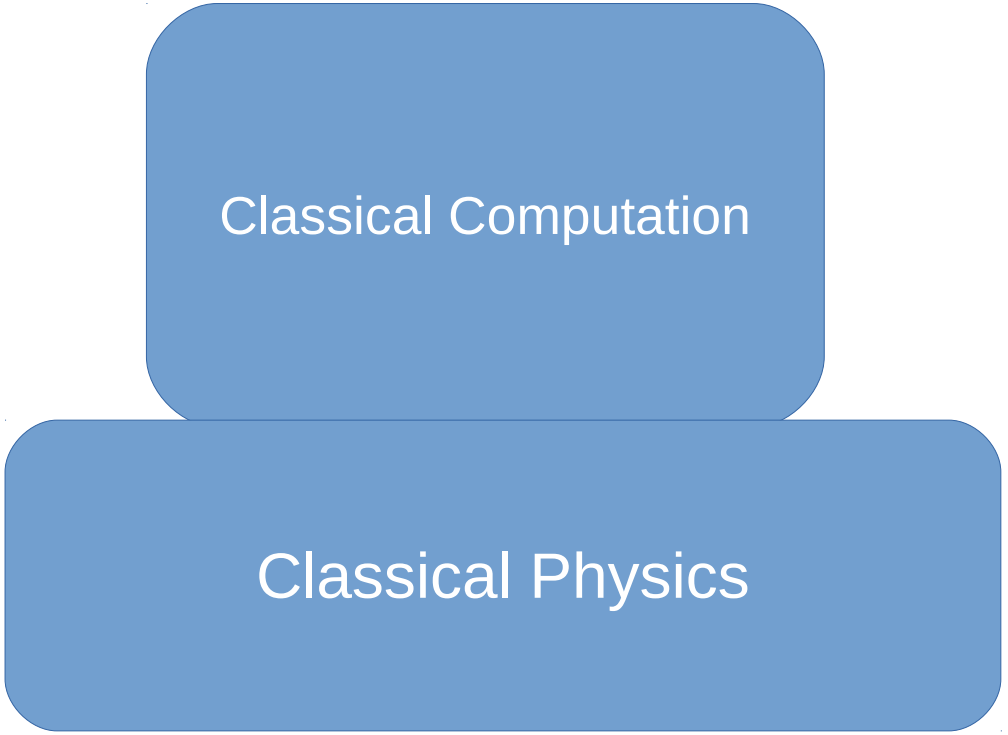
Postulate I
Ket keeps all available information on a system

Postulate II
Observables are related to operators acting on kets

Postulate III
Measurement collapses information
Born rule dictates this probabilistic collapse

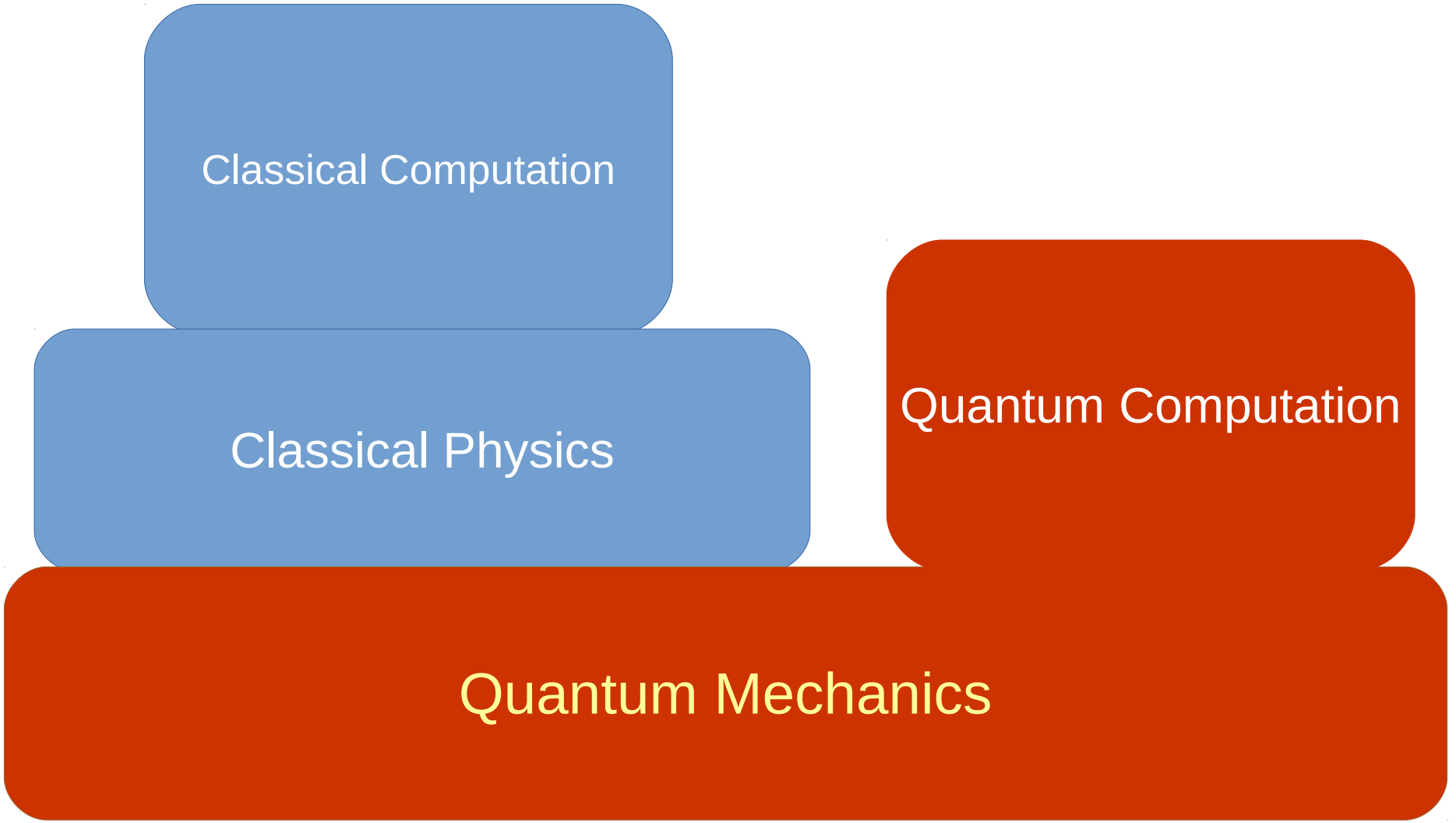
Postulate IV
Evolution is unitary and deterministic, keeps probabilities

Information ➡ QM



Church, Post, Turing,...: Computing = Physics

Information ➡ QM



Feynman: Computing with QM

Physics

Logical bit

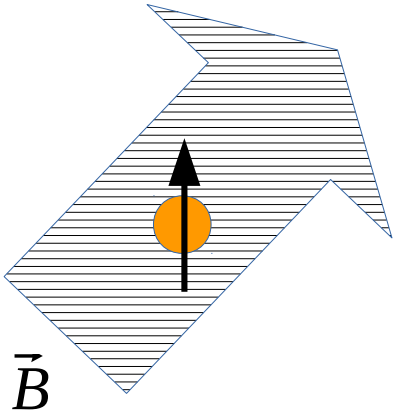
$|0\rangle$

$|1\rangle$

Superposition

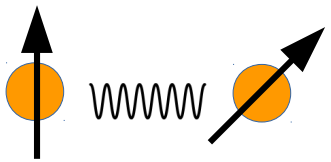
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Unitary Evolution = Quantum Gates



$$U_H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$U_H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$



$$U_{CNOT}|00\rangle = |00\rangle \qquad U_{CNOT}|10\rangle = |11\rangle$$

$$U_{CNOT}|01\rangle = |01\rangle \qquad U_{CNOT}|11\rangle = |10\rangle$$

New Logical Gates

Interference

Quantum advantatge

Massive superpositions for computation!

$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} \left| i_1, i_2, \ldots, i_n \right\rangle$$

2^n superpositions on ***n*** qubits

1 register of 50 qubits contains more information than any classical computer

Massive parallel computation!

$$U|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} U \left| i_1, i_2, \ldots, i_n \right\rangle$$

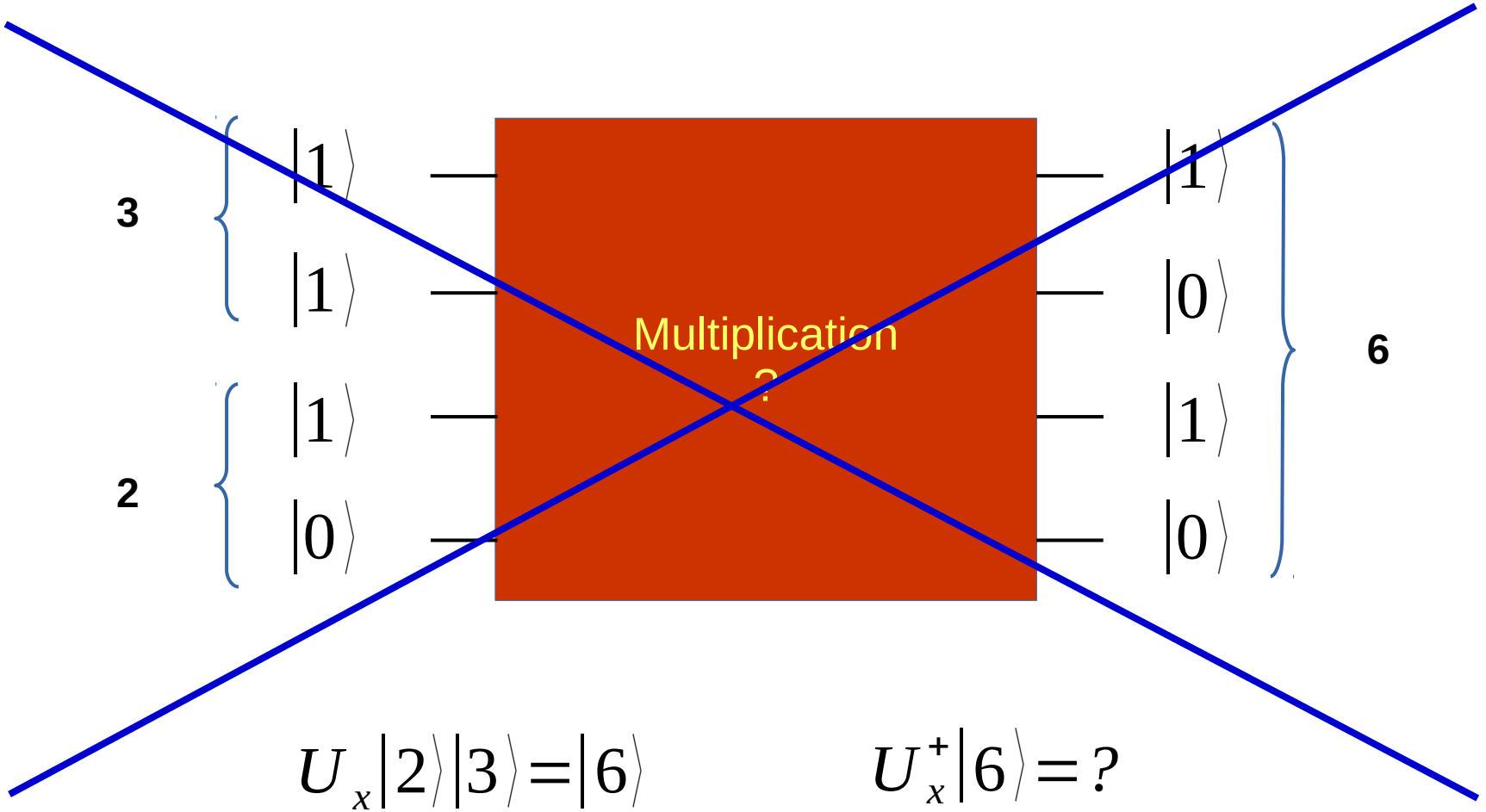
BUT

Quantum Mechanics follows its on laws

Multiplication

$$U_x|2\rangle|3\rangle=|6\rangle$$

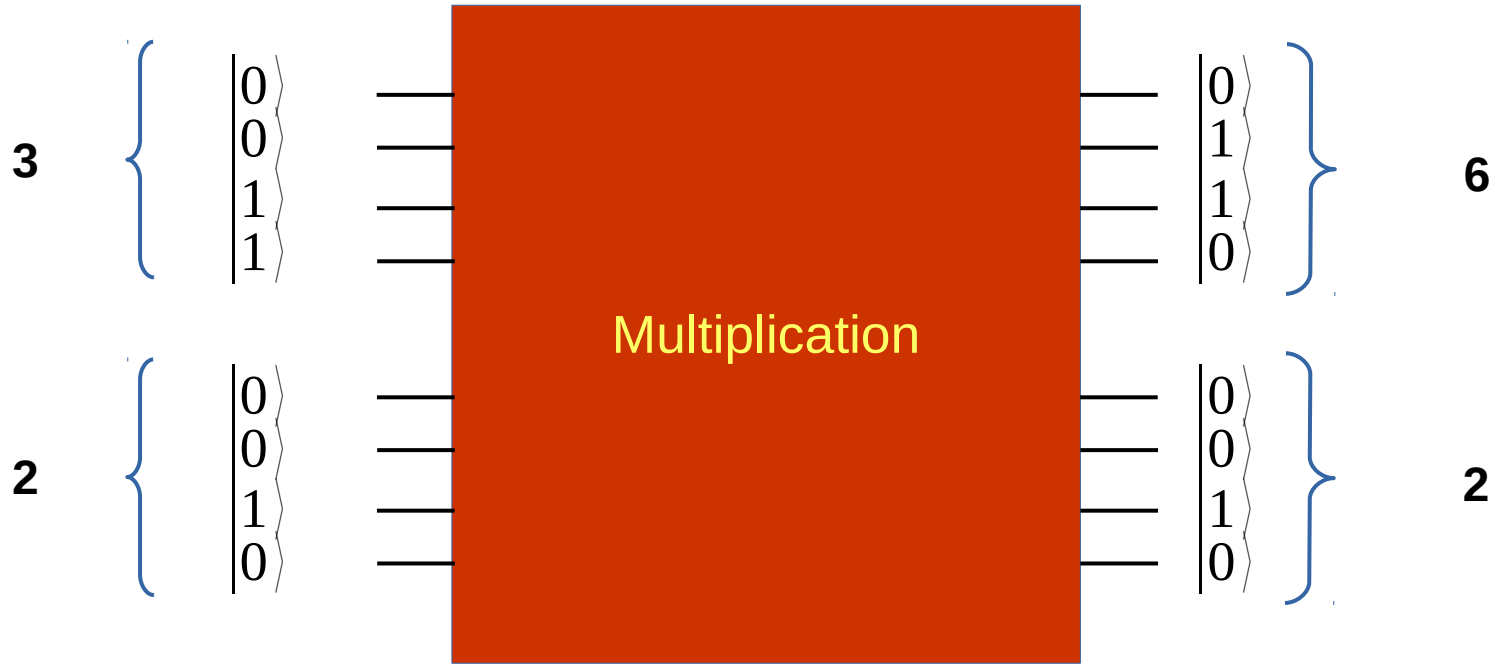
Multiplication



$$U_x|2\rangle|3\rangle = |6\rangle \qquad U_x^+|6\rangle = ?$$

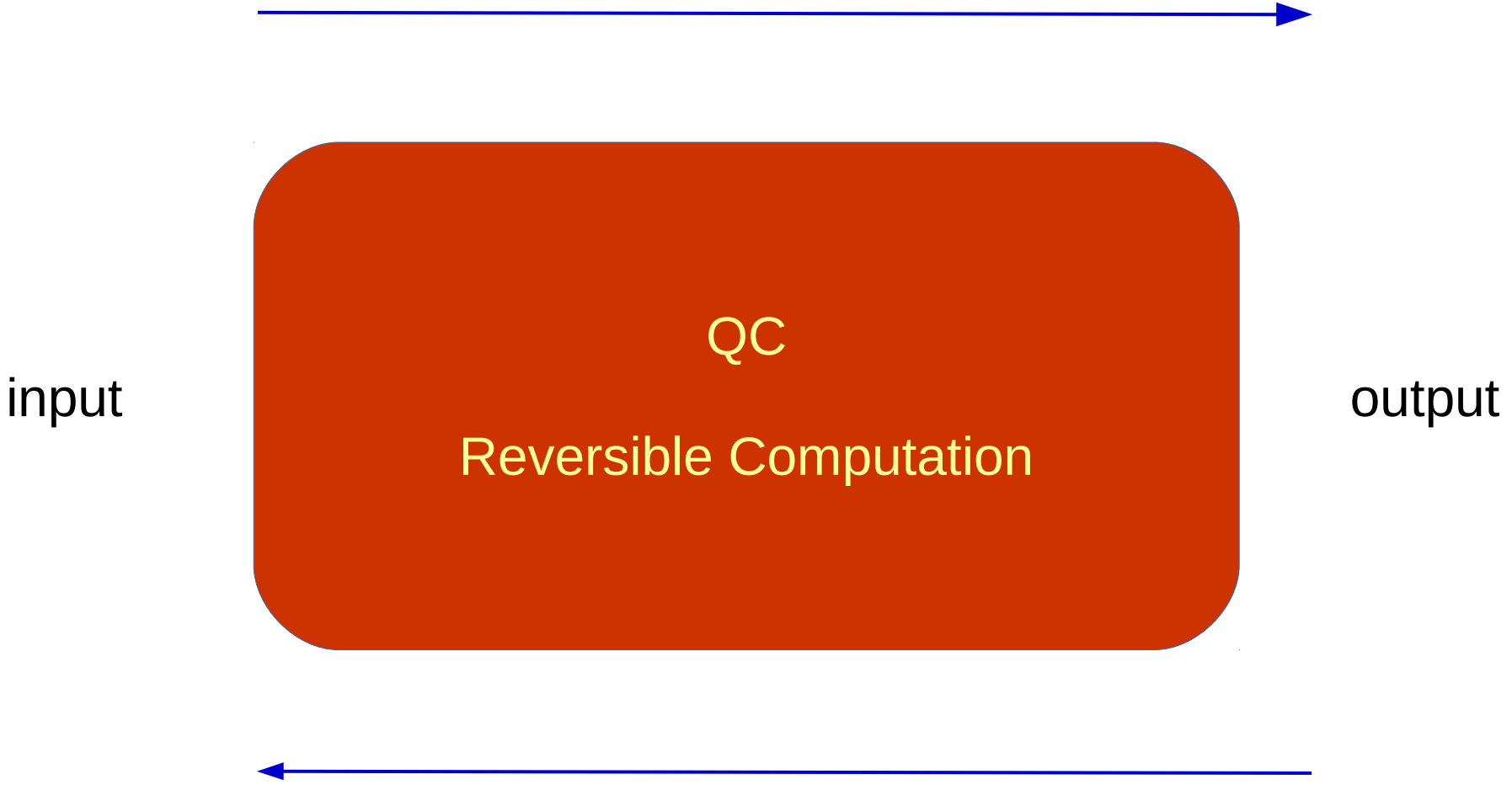
NOT UNITARY

Unitarity = Reversible Computation

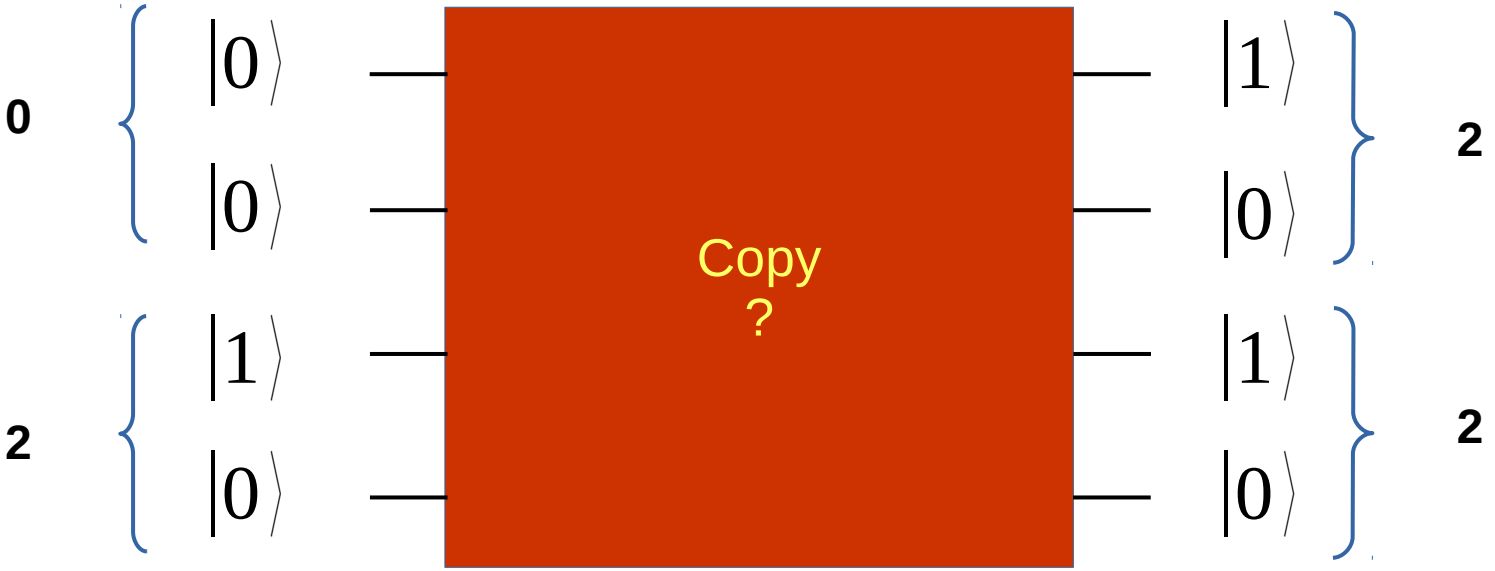


$$U_x|2\rangle|3\rangle = |2\rangle|6\rangle$$

$$U_x|x\rangle|y\rangle = |x\rangle|f(x,y)\rangle$$

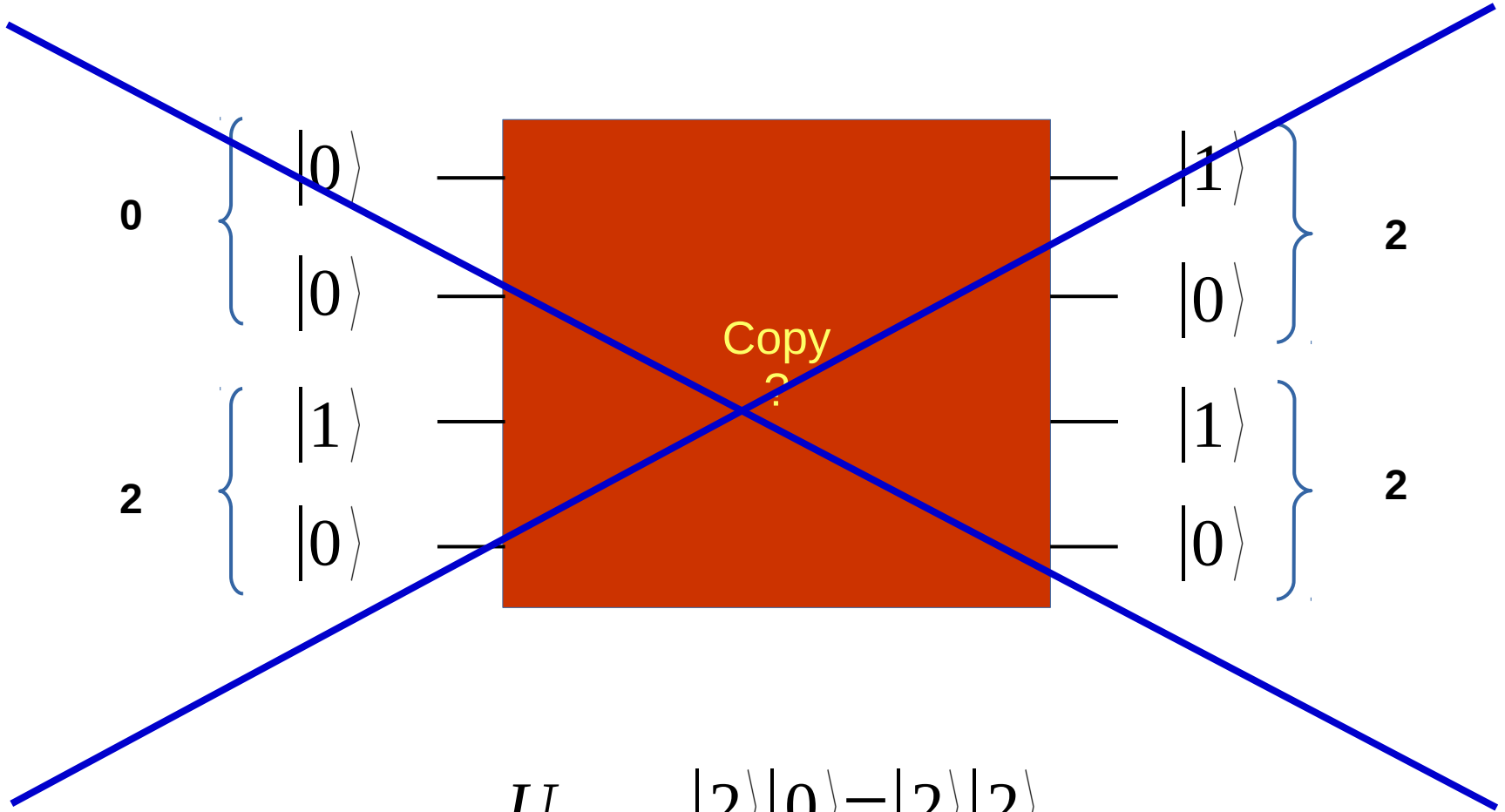

input
QC
Reversible Computation
output

Copy



$$U_{cloning}|2\rangle|0\rangle=|2\rangle|2\rangle$$

Copy



$$U_{cloning}|2\rangle|0\rangle=|2\rangle|2\rangle$$

NO CLONING

No cloning theorem

$$U_{cloning}|0\rangle|a\rangle=|0\rangle|0\rangle$$
$$U_{cloning}|1\rangle|a\rangle=|1\rangle|1\rangle$$

$$U_{cloning}(c_0|0\rangle+c_1|1\rangle)|a\rangle=c_0|0\rangle|0\rangle+c_1|1\rangle|1\rangle$$

$$\neq(c_0|0\rangle+c_1|1\rangle)(c_0|0\rangle+c_1|1\rangle)$$

No cloning underlies

- no inference for the exact result of a measurement
- no violation of causality
- no breaking quantum cryptography,….

Measurement

Inherent quantum randomness

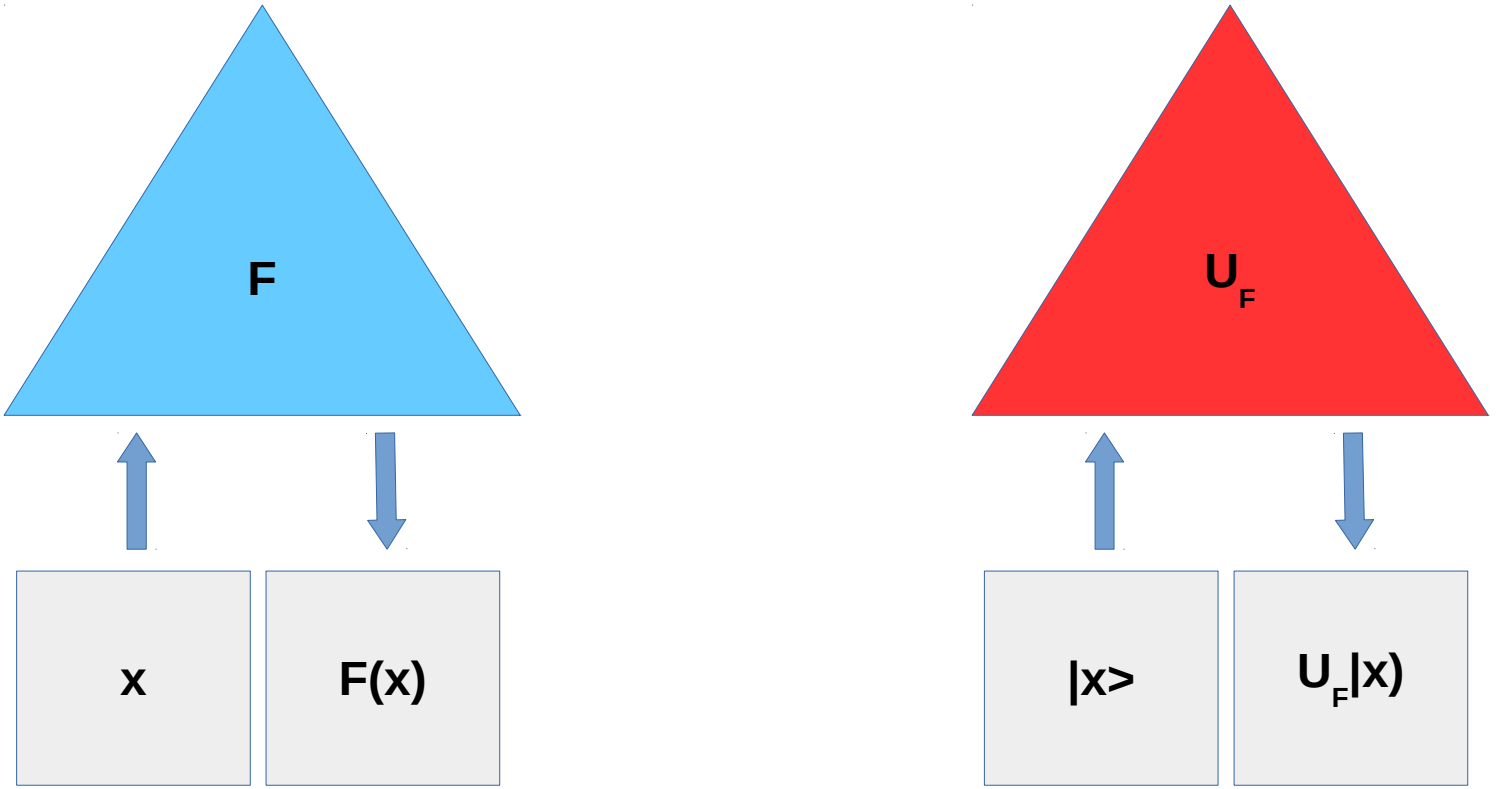
$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n} c_{i_1, i_2, \ldots, i_n} \left| i_1, i_2, \ldots, i_n \right\rangle$$

$$P\left(i_1, i_2, \ldots, i_n\right) = \left| c_{i_1, i_2, \ldots, i_n} \right|^2$$

The magic of

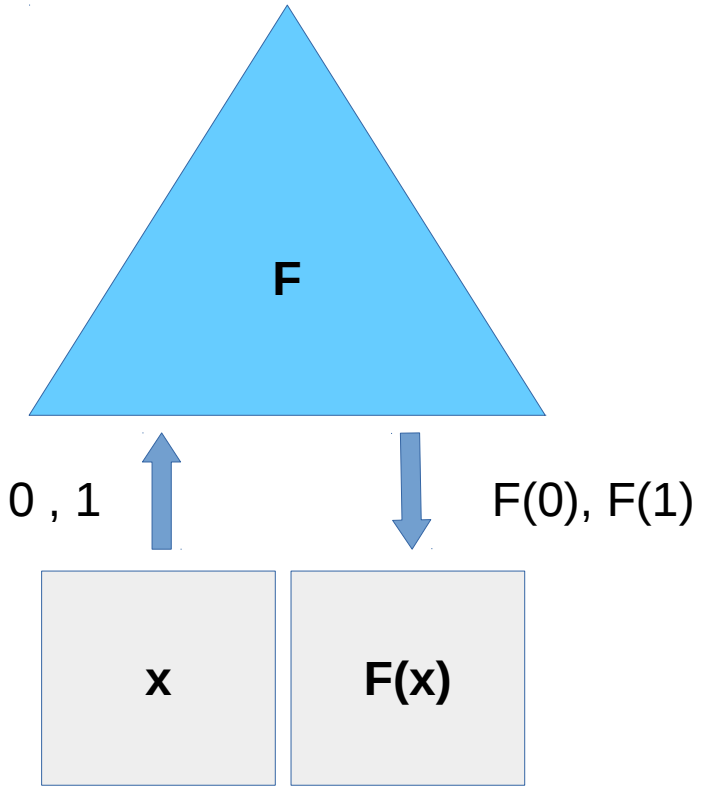
Quantum Algorithms

Queries to an **oracle**



Can QM reduce the number of calls to an oracle?

Queries to an **oracle**



Simplest example: is F constant?

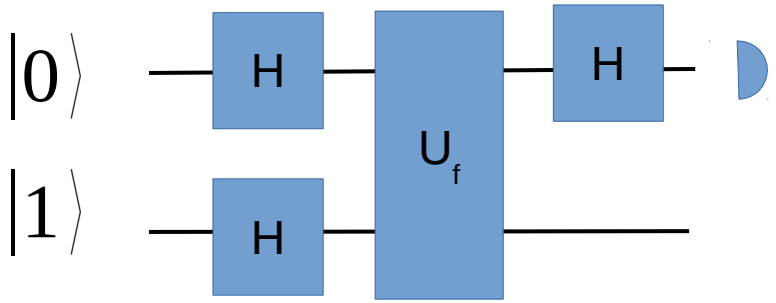
$$F:\{0,1\}\rightarrow\{0,1\}$$

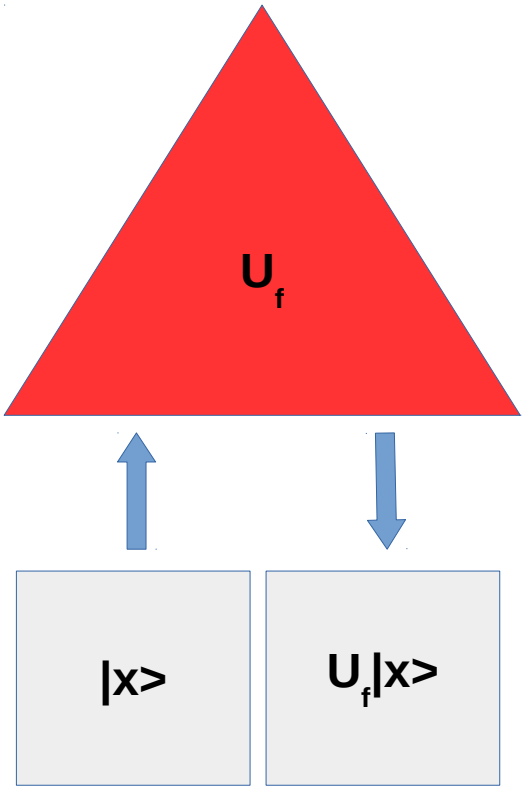
$$F(0)=F(1)\,?$$

$$F(0)\neq F(1)\,?$$

Classically, we need two calls to know if F is balanced

Queries to an **oracle**





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

$$(|0\rangle+|1\rangle)(|0\rangle-|1\rangle)$$

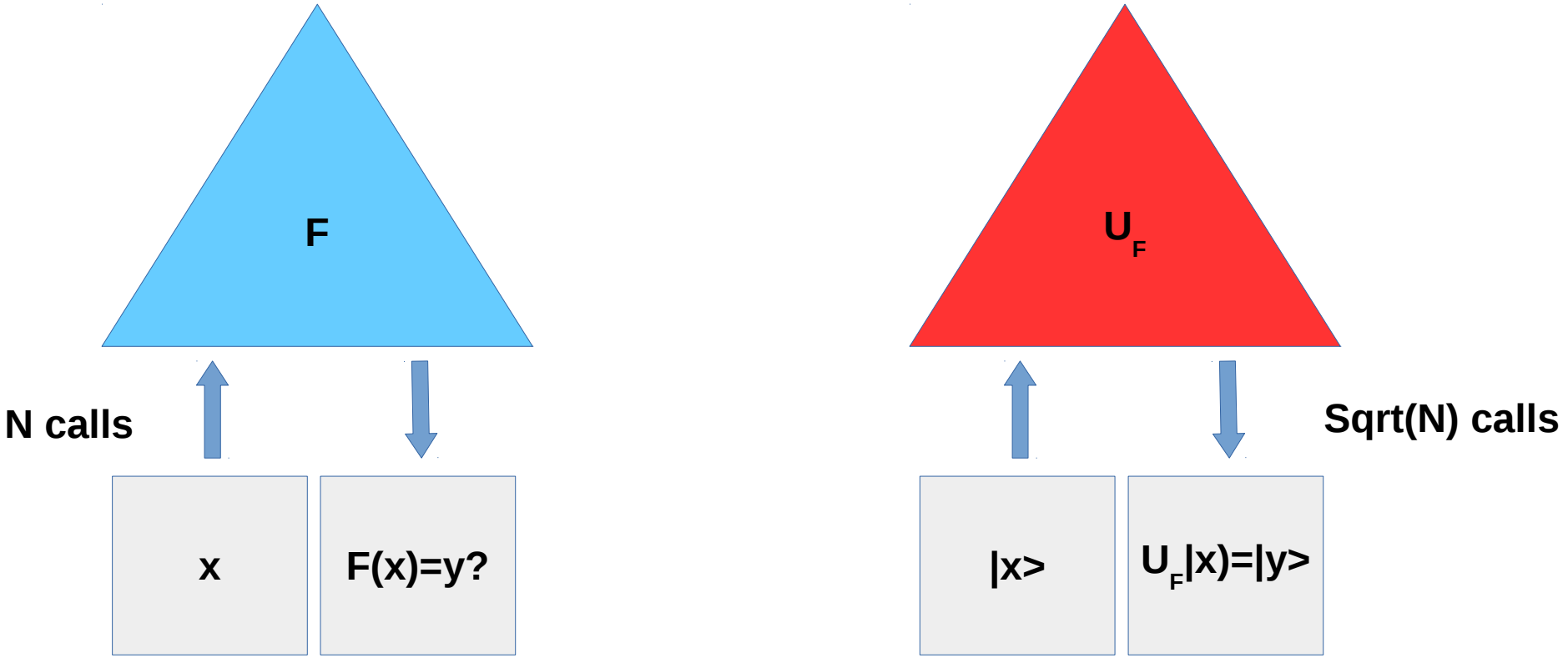
$$|0\rangle(|0+f(0)\rangle-|1+f(0)\rangle)+|1\rangle(|0+f(1)\rangle-|1+f(1)\rangle)$$

$$(|0\rangle+(-1)^{f(0)+f(1)}|1\rangle)(|0\rangle-|1\rangle)$$

$$(1+(-1)^{f(0)+f(1)})|0\rangle+(1-(-1)^{f(0)+f(1)})|1\rangle$$

QM needs a single call to the oracle!!

Queries to an oracle: **search an unstructured database**



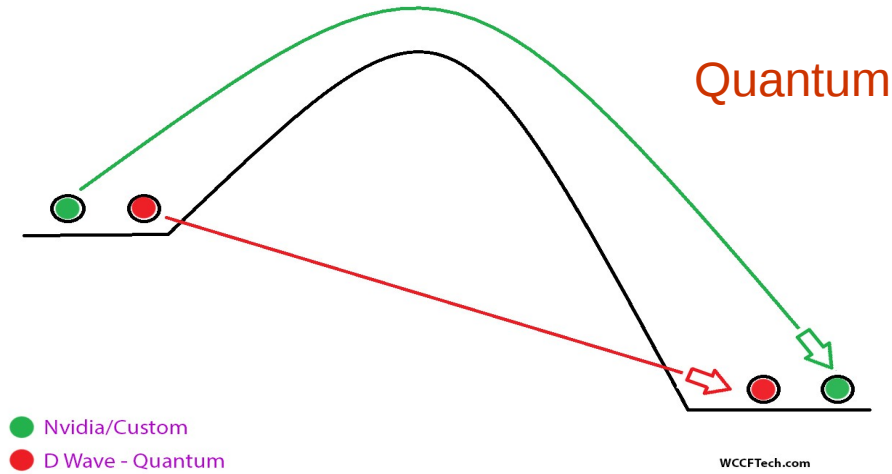
Grover's algorithm

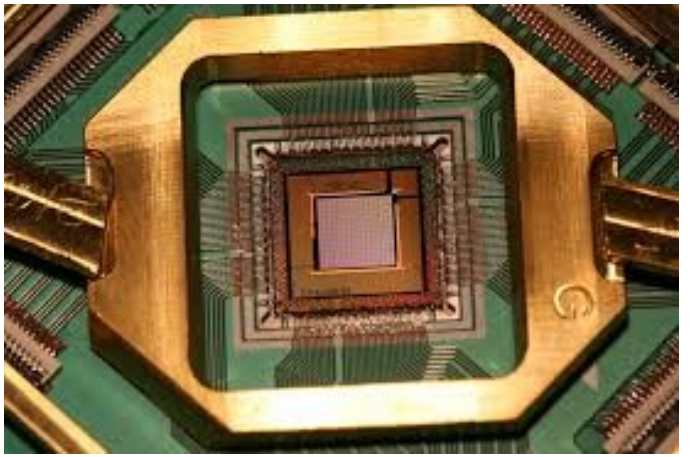
Solve a hash, bitcoin!

Annealing

DWAVE-2 2048 qubits
Optimization problems, no error correction 12M/machine

Tunnel across the barrier!!





$$H = \sum_{ij} J_{ij} z_i z_j$$

Optimization problems

Factorization

$$N = p\,q$$

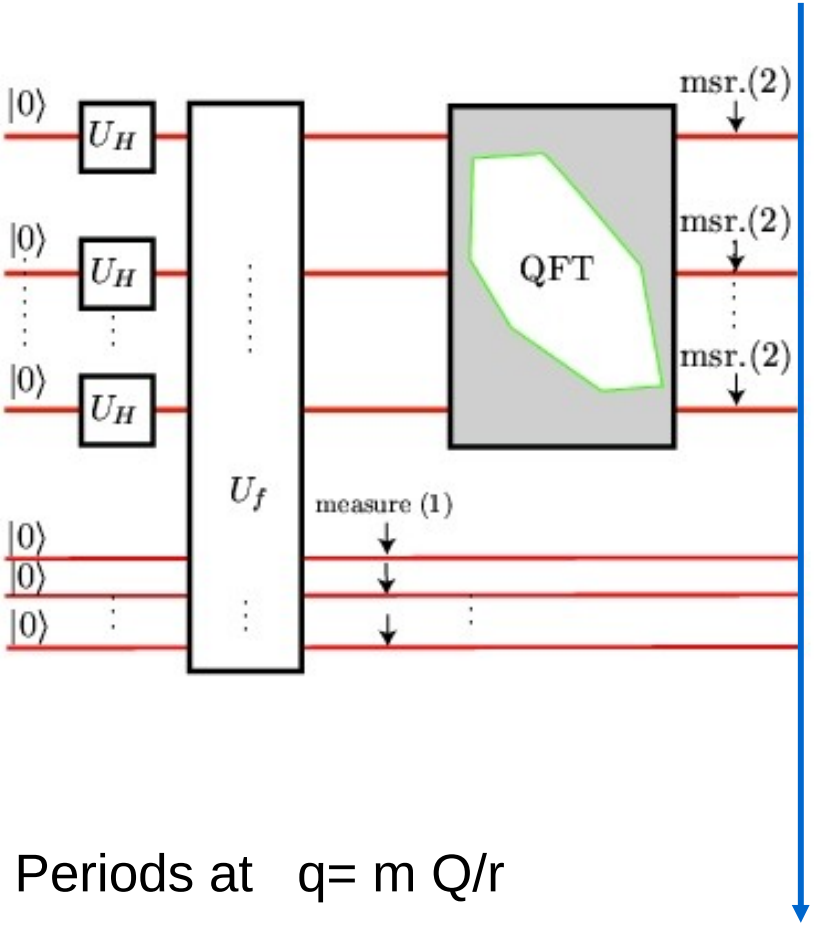
Choose a and find r such that $a^r = 1 \bmod(N)$

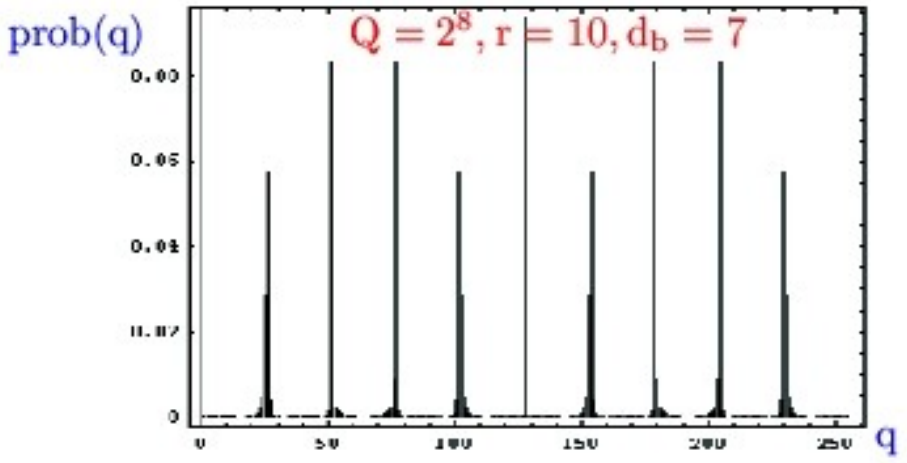
i) r is not even
ii) r is even and $a^{r/2} = -1 \bmod(N)$
iii) r is even and $a^{r/2} \neq -1 \bmod(N)$

If iii) $p = \gcd(N, a^{r/2} + 1)$ $q = \gcd(N, a^{r/2} - 1)$

Factoring = Finding a hidden period

$$P(q) = \frac{1}{QB}\left|\sum_{k=0}^{B-1} e^{iqr\,2\pi/Q}\right|^2$$





Periods at q= m Q/r

read r

Factorization (Quantum Fourier Transform)

Classical Computer

$$e^{\left(\frac{64}{9}\right)^{1/3} n^{1/3} (\log n)^{2/3}}$$

Quantum Computer

$$n^3 (\log n)(\log(\log n))$$

Quantum exponential speedup
Breaking of RSA, Discrete log, Eliptic curve

Connectivity

NSA Says It "Must Act Now" Against the Quantum Computing Threat

The National Security Agency is worried that quantum computers will neutralize our best encryption – but doesn't yet know what to do about that problem.

New algorithms

Quantum Algorithms

Known circuits

Search - Grover
QFT - Shor
Deutsch

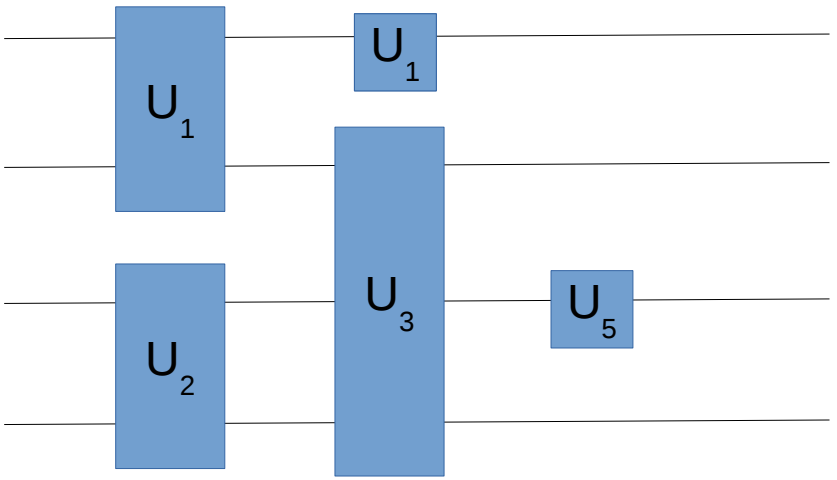
Annealing

Direct Annealing
Adiabatic Evolution

Variational

Autoencoders
Eigensolvers
Classifiers

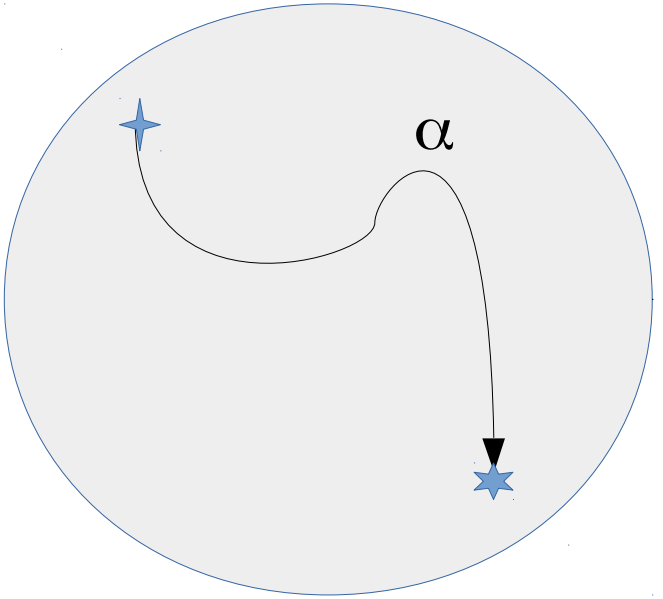
Variational circuits



$$U(\vec{\alpha}) = U_n \ldots U_2 U_1$$

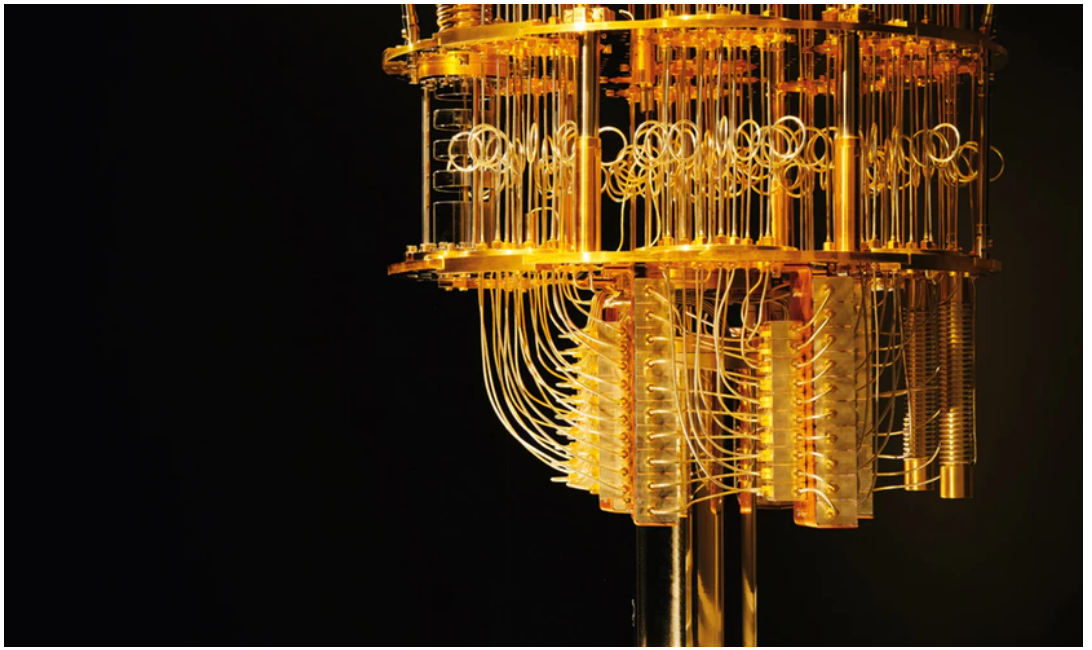
Delivers quantum states

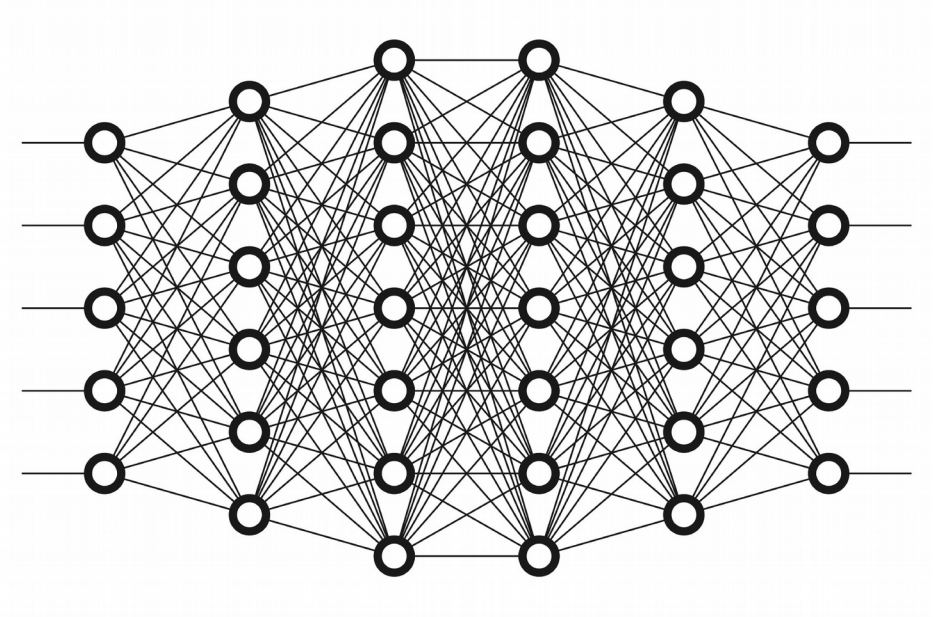
Explores a large (Hilbert) space

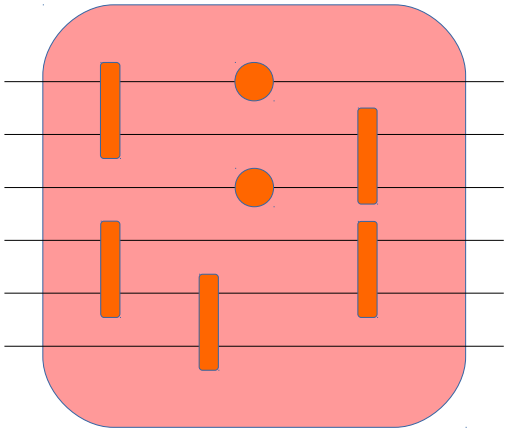


Classical characterization of a global unitary

Qcomputer is a machine to generate variational states





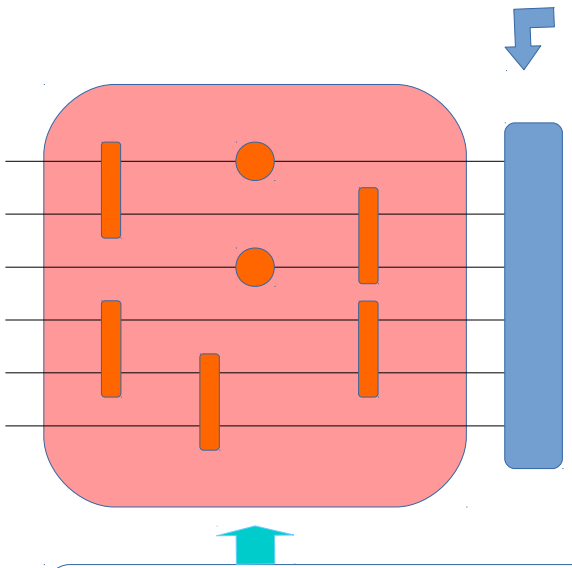


Processing by hidden neurons

Processing by superpositions

Variational Quantum Eigensolvers

Aspuru-Guzik
Zapata Computing



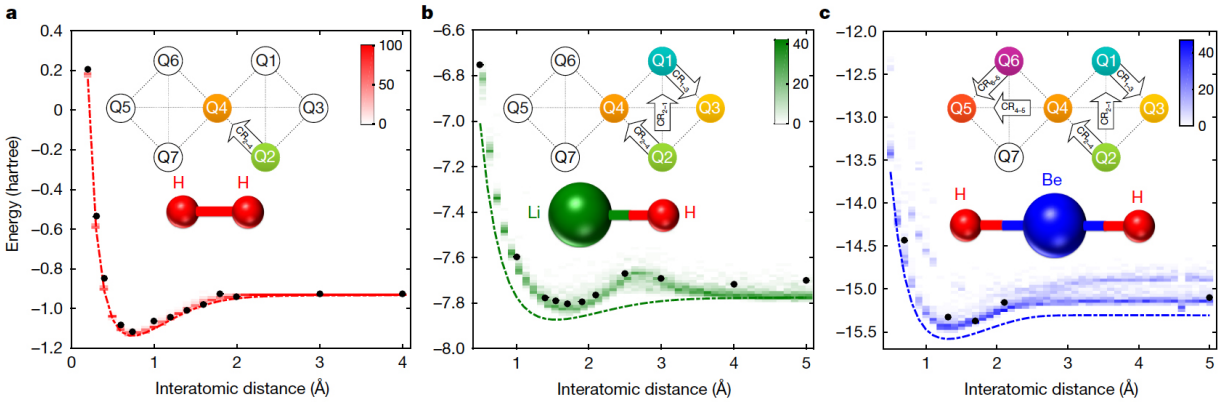
any optimization problem

Read out

Machine learning
on circuit design

Energy
Correlations
Classical & Quantum

First applications
Quantum Chemistry!



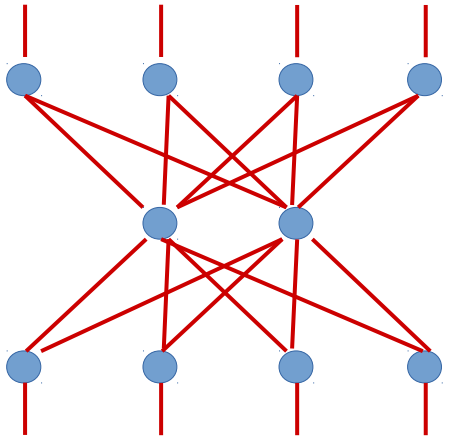
Detect a relevant subspace in data

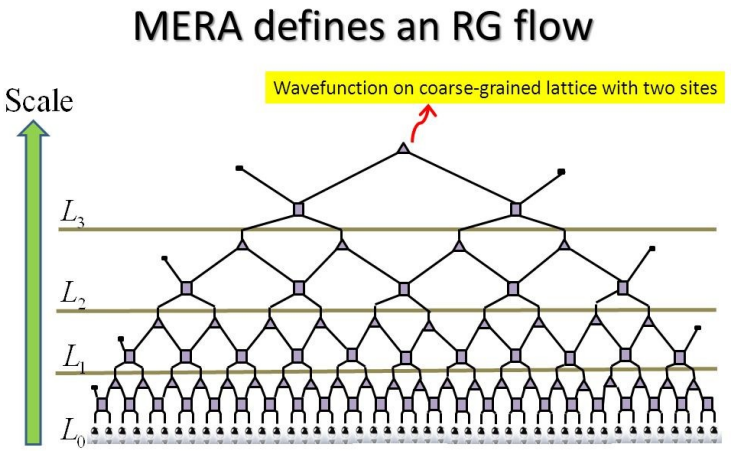
Compressor

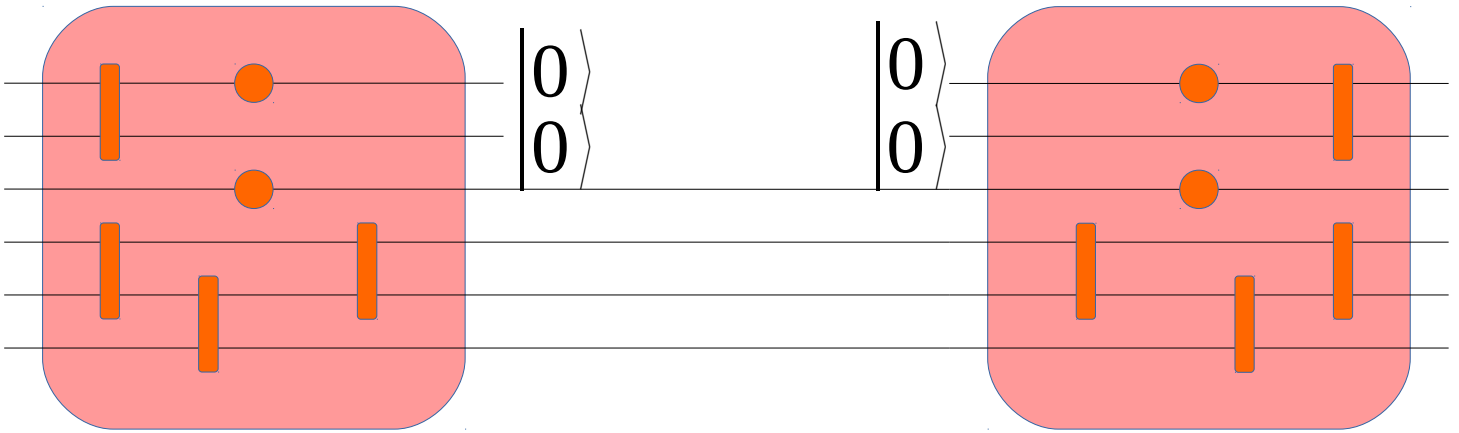
Generate patterns

Autoencoder

I =



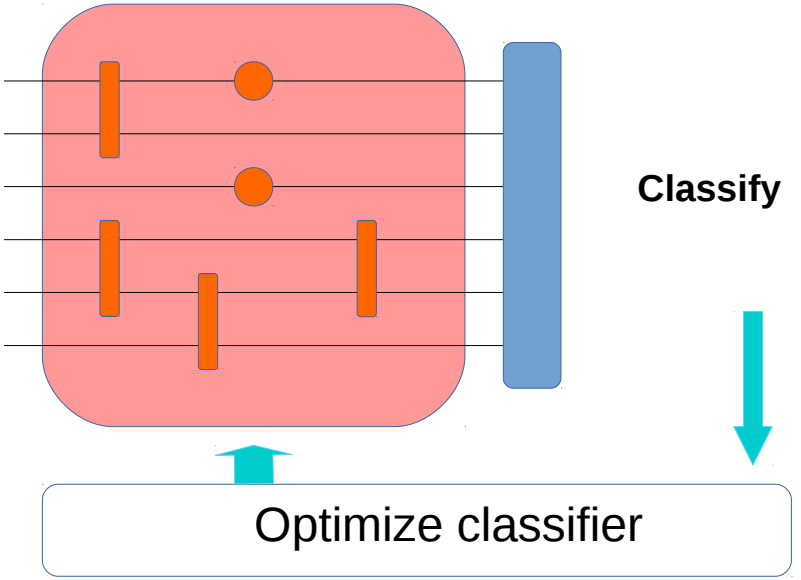


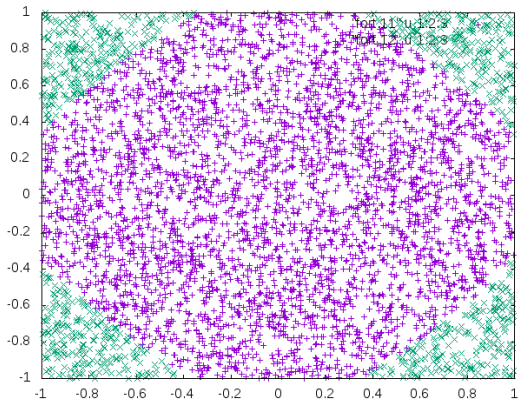


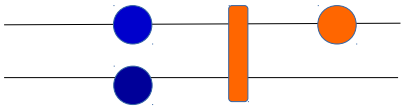
Quantum Classifier

$$U(\vec{\alpha})$$

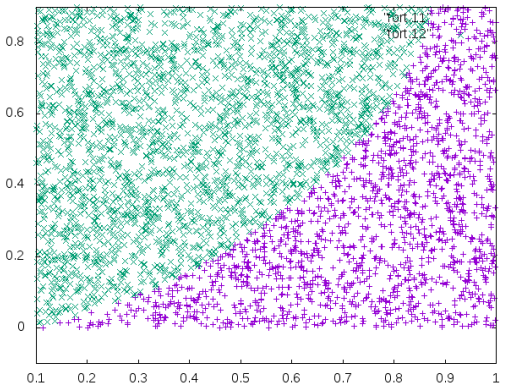
Codify data in gates





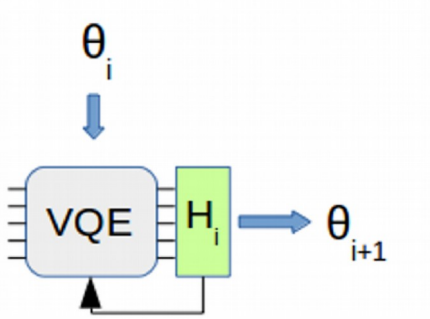


97% success



Adiabatically Assisted Variational Quantum Eigensolver

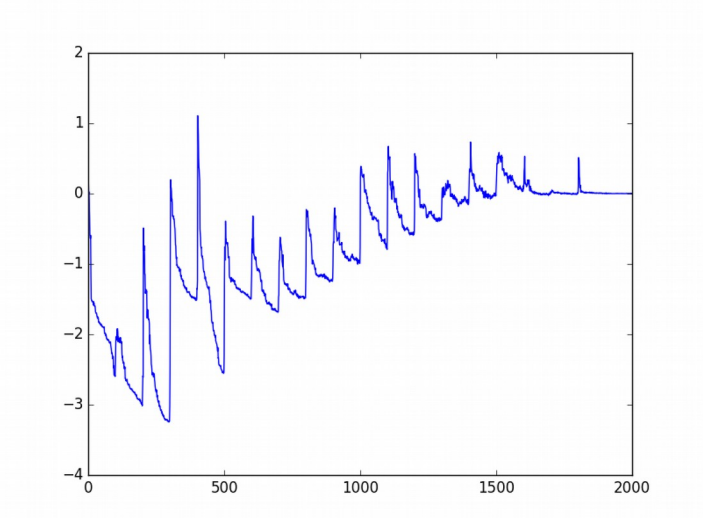
$$H(s) = (1-s)H_0 + s\,H_P$$



i) Find circuit for ground state H_0, s=0, with VQE.

ii) Increase s, solve new H(s) with VQE using as initial condition the previous circuit.

Iii) Reach H_P



AA shows a path around local minima

Solves hard instances of
Exact Cover (NP-complete)

VQE fails

CONCLUSION

Quantum advantatge
- Speed, Size, **Energy**

Quantum Race
- **Quantum supremacy**
- Factorization
- (post)Quantum cryptography

Quantum Algorithms
- Variational
- Machine learning on **pulses**

IDEAS

Use adiabatic evolution of chi2

$$chi^2 = (1-s)\,chi_o^2 + s\,chi_P^2$$

Closure data based on smooth wiggle-less pdfs

Interpolate from other pdf distributions to ours?

Explore minimization to train neural networks

BCN QUANTIC QILIMANJARO

1 qubit-qutrit

Classifier
Boltzmann machine