A quantum machine learning future:

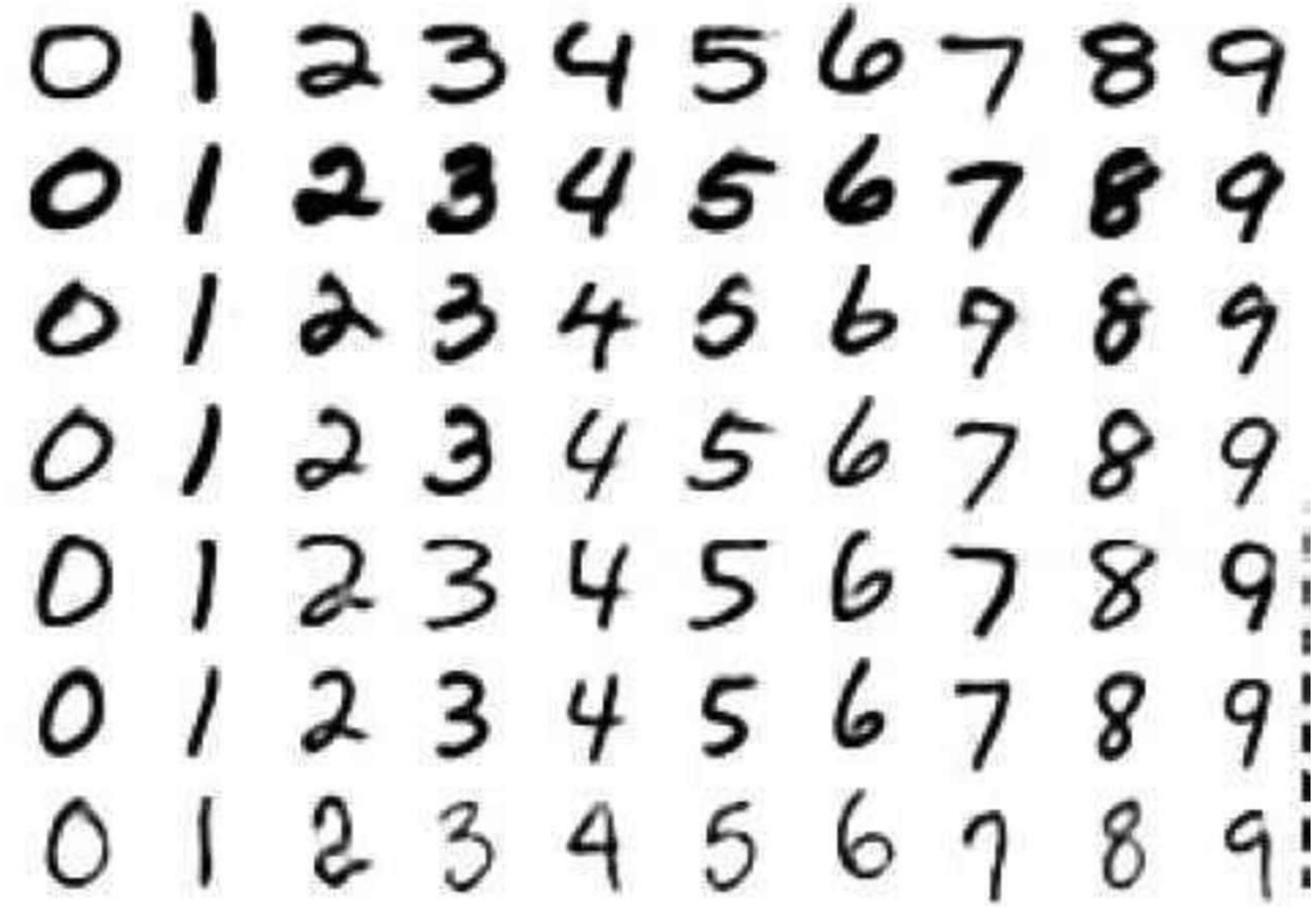
How quantum algorithms will change IT

32° Convegno Nazionale AIEA - Associazione Italiana Information Systems Auditors

Alessandro Luongo

https://luongo.pro

@scinawa

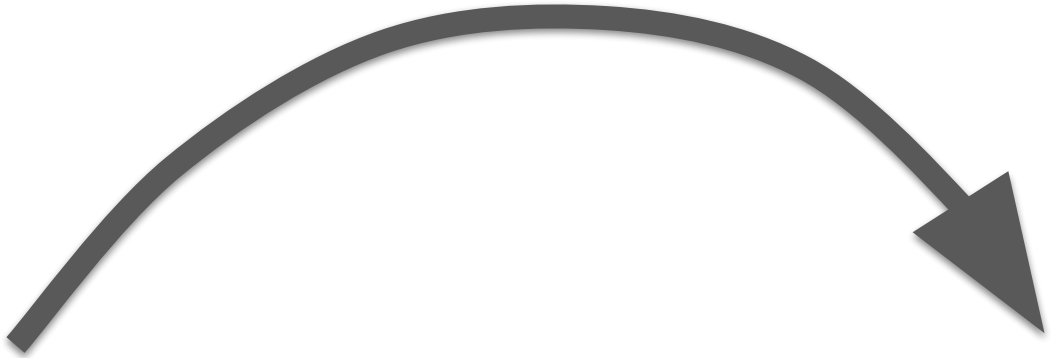


What time are we living in?

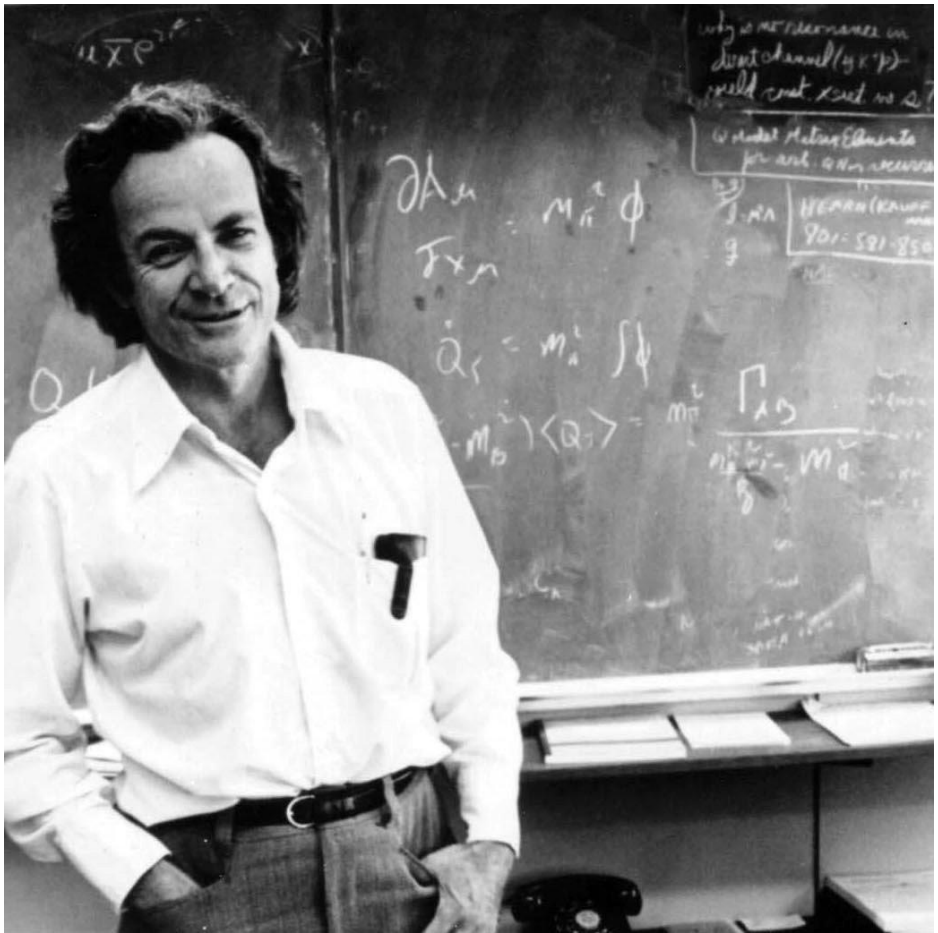
- 1960: The **first** quantum revolution: **exploit** laws that govern physical reality (lasers, MRI, ...)
- NOW: the **second** quantum revolution: **actively use** the rules of QM to develop new technologies

Classical mechanics

$$x = x_0 + v_0 t \qquad y = -\frac{1}{2} g t^2 + v_{0_y} t + y_0$$



Can we simulate physics with (classical) computers?



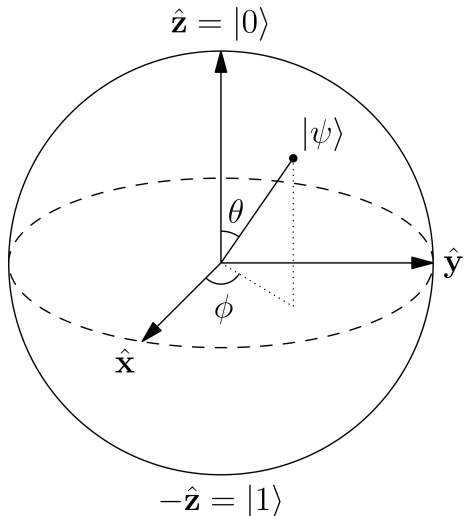
(We believe not)

Introduction to quantum computation (1)

- **Def**: A qubit is a unit vector in a 2-dimensional space (over complex number)

$$|\psi\rangle = [a, b] \qquad |a|^2 + |b|^2 = 1 \qquad a, b \in \mathbb{C}$$

$$|CAT\rangle = \frac{1}{\sqrt{2}}|DEAD\rangle + \frac{1}{\sqrt{2}}|ALIVE\rangle$$



How to compose qubits? (2)

$$|\psi\rangle = [a, b] \quad |\phi\rangle = [c, d]$$

$$|\psi\rangle \otimes |\phi\rangle = [ac, ad, bc, bd]$$

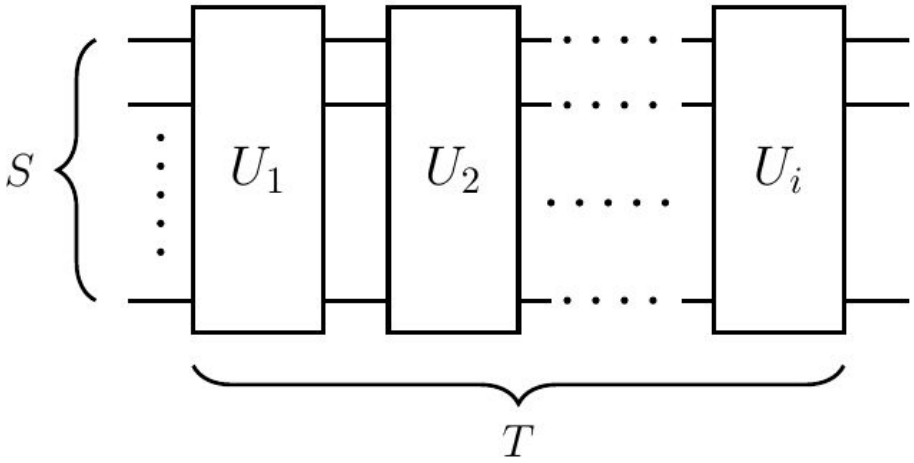
$$|\psi\rangle = \sum_{\{0,1\}^n} \alpha_i |i\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

Non possiamo simulare più di 50 qubits.

Computations as rotations… (3)

$$UU^\dagger = U^\dagger = I$$

$$U^{-1} = U^\dagger$$



$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$X|0\rangle = |1\rangle \quad X|1\rangle = |0\rangle$$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$CNOT\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle$$

$$CNOT\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle$$

First source of speedups: Grover's algorithm(s).

Problem: find right one among **n** boxes.

Classically $O(n)$

Quantumly ... $O(\sqrt{n})$

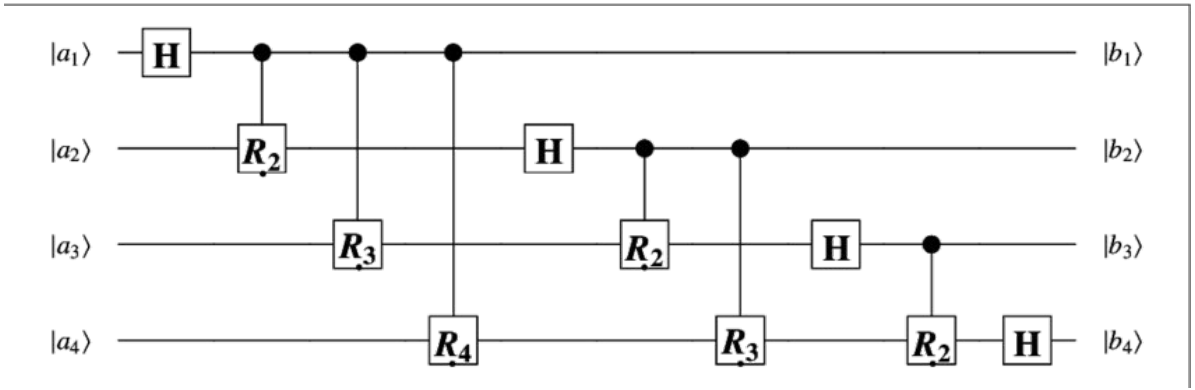
- 1.000.000 operations -> 1000 operations
- 7 days -> 2.5 days

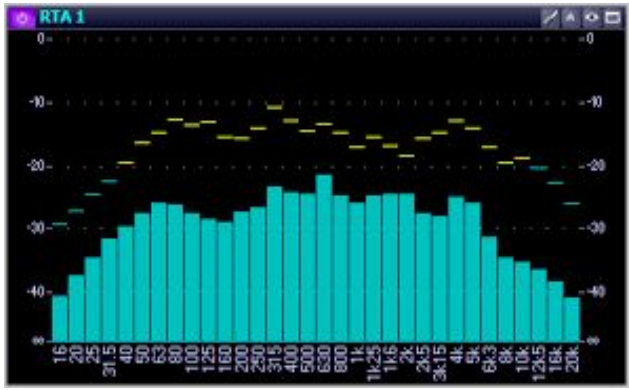
Second source of speedup: Quantum Fourier Transform

Classically: $O(n \log n)$

Quantumly: $O(\cancel{n} \log n)$

QFT is the "origin" of the exponential speedups.





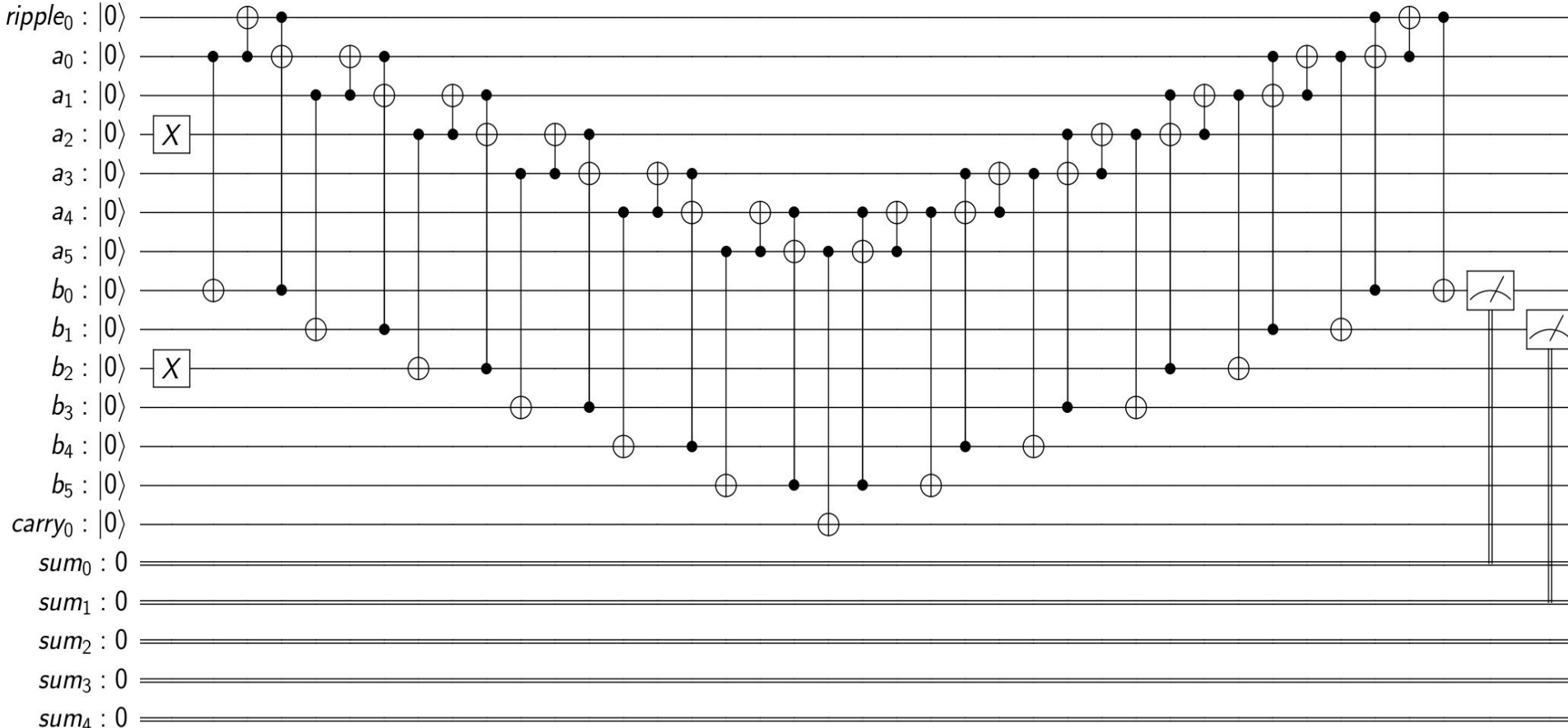
"Hey Scinawa, math is cool…
but in practice?"

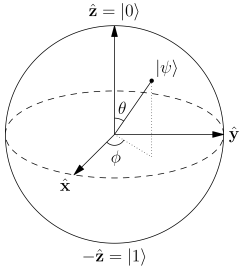
```
a = 4
b = 4

n = max([len(bin(a)[2:]), len(bin(b)[2:]) ])+3

print(n)
program_types_spec = {
    "circuits": [{
        "name": "Quantum-Adder-circuit",
        "quantum_registers": [

        { "name": "ripple",
          "size": 1},

       { "name": "a",
          "size": n},

        { "name": "b",
          "size": n},

        { "name": "carry",
          "size": 1}

        ],
        "classical_registers": [
            {"name": "sum",
              "size": n},
            {"name": "carrysum",
            "size": 1},

        ]
    }],
}
```

```
qp = QuantumProgram(program_types_spec)
qc = qp.get_circuit("Quantum-Adder-circuit")

qr_b = qp.get_quantum_register("b")
qr_a = qp.get_quantum_register("a")
q_ripple = qp.get_quantum_register("ripple")
q_carry = qp.get_quantum_register("carry")
c_sum = qp.get_classical_register("sum")
c_carrysum = qp.get_classical_register("carrysum")


qmalt.utils.initialize_index(qc, qr_a, a)
qmalt.utils.initialize_index(qc, qr_b, b)

Adder.apply(qc, q_ripple, qr_a, qr_b,  q_carry)

qc.measure(qr_b, c_sum)
```

```
def apply(self, ripple, a, b, carry):
    """
    A simple ripple carry adder (no optimizations)

    :param self: quantum circuit
    :param ripple: quantum register of 1 qubit
    :param x: n qubit quanntum register
    :param y: n qubit quantum register
    :param carry: quantum register of 1 qubit
    :return: None
    """
    assert a.size == b.size
    assert ripple.size == carry.size == 1

    n = a.size
    majority(self, ripple[0], b[0], a[0])

    for j in range(n - 1):
        print("1){} a[{}], b[{}], a[{}]".format(j, j, j+1, j+1))
        majority(self, a[j], b[j+1], a[j+1])

    self.cx(a[a.size-1], carry[0])

    for j in range(n - 2, -1, -1):
        print("2){} a[{}], b[{}], a[{}]".format(j, j, j+1, j+1))
        unmajority(self, a[j], b[j+1], a[j+1])

    unmajority(self, ripple[0], b[0], a[0])
```

X a[2]
X b[2]
CNOT a[0], b[0] ….





Hybrid quantum-classical computation

"Quantum" as a GPU

Write code (python like) → Compile into QASM → Apply ECC → Translate into HW-QASM →


CHANGE
For The Better

Computer security

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

By: JP Aumasson, @veorq

Some work in progress

- Malware detection
- Formal software verification (model checking)
- Quantum Firewalls

Quantum chemistry!

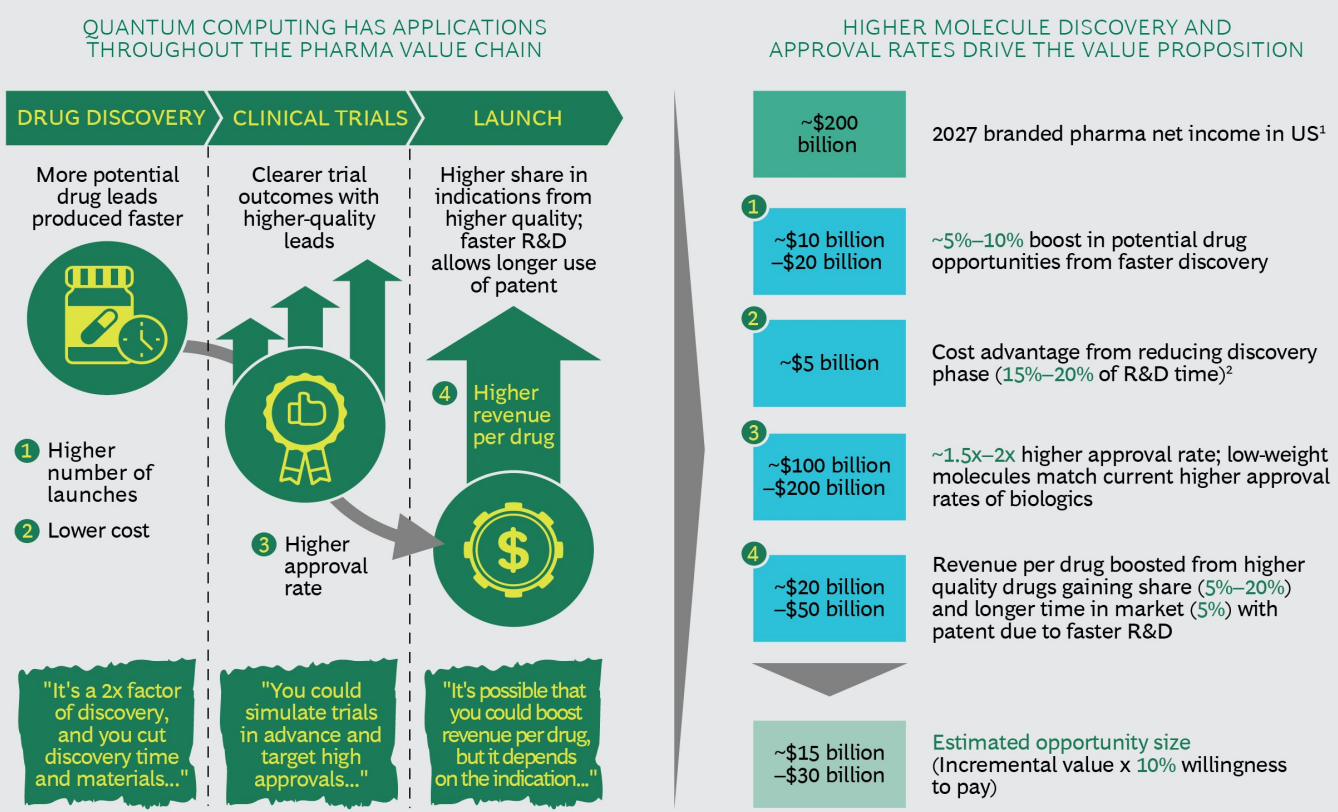
- Addressable market $20+ billion.
- Rate of drug discovery + 5% to 10%.
- Development times + 15% to 20%.
- Better molecule design increase approval rates 1.5x or 2x.

What about new materials?

- Addressable market up to $7 billion by 2030.

Forecast by 2030. Source: BCG Coming quantum computing leap
https://www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx

EXHIBIT 2 | Complex Molecule Discovery in Pharma R&D Could Be a $15 Billion to $30 Billion Market Opportunity



Sources: Statistica reports; Wired; Lawrence Livermore National Laboratory; Motherboard; Fierce Biotech; expert interviews; BCG analysis.
[1]Assumes 7% CAGR in line with historical trends, 30% net margin, and 75% of total pharma market branded. [2]Reduces ~25% of drug discovery, itself 15% to 20% of R&D, which represents ~17% of revenue.

Source: BCG Coming quantum computing leap https://www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx

Ammonia Based Fertilizer: The $11 Billion Problem Seeking a Solution

https://quantumcomputingreport.com/our-take/ammonia-based-fertilizer-the-11-billion-problem-seeking-a-solution/

Quantum Machine Learning

Remember: Machine Learning is just Linear Algebra.

Our dataset is a matrix $X \in \mathbb{R}^{n \times d}$

Classical algorithms to perform linear-algebraic operations on matrices take $O(n^2 d)$

Problem: what if data we produce double every 2 years?

We need quantum!

Note...quantum mechanics is all about matrices and vectors!

- Breakthrough paper in 2009 for matrix inversion
- Successively improvements till 2018
- Assume existence of QRAM

Theorem (informal) - Quantum Linear Algebra
There are efficient quantum algorithms that, given a matrix M and a vector x stored in QRAM

- Multiply a vector by the inverse of M
- Multiply a vector by M
- Project x onto a subspace of eigenvectors of M.

Slow Feature Analysis

$$\vec{x}(t) = [x_1(t), x_2(t)...x_d(t)] \longrightarrow \vec{y}(t) = [y_1(t), y_2(t)...y_k(t)]$$

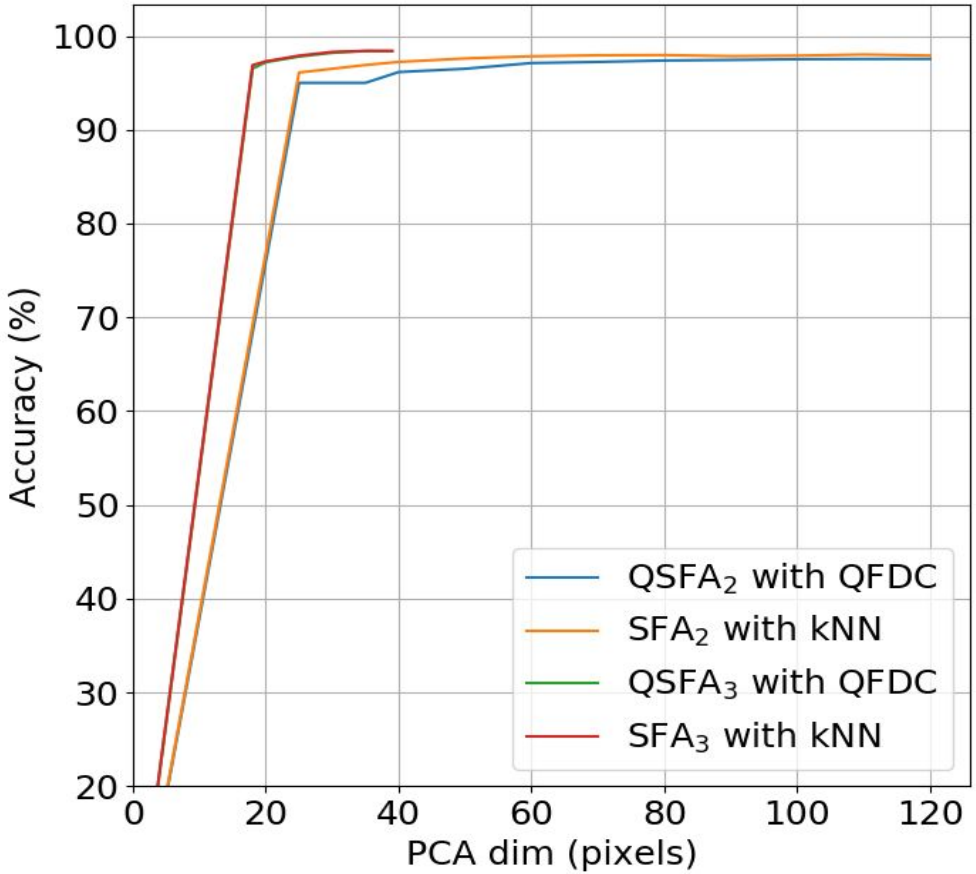
$$\vec{y}(t) = [g_1(\vec{x}(t)), g_2(\vec{x}(t)), ...g_k(\vec{x}(t))]$$

With constraints:

- Average of the components of output signal is 0
- Variance of the components of output is 1
- Signals are decorrelated

Quantum Slow Feature Analysis

Theorem 6 (QSFA algorithm). *Let* $X = \sum_i \sigma_i u_i v_i^T \in \mathbb{R}^{n \times d}$ *and its derivative matrix* $\dot{X} \in \mathbb{R}^{n \log n \times d}$ *stored in QRAM as described in Appendix A. Let* $\epsilon, \theta, \delta, \eta > 0$. *There exists a quantum algorithm that produces as output a state* $|\overline{Y}\rangle$ *with* $||\overline{Y}\rangle - |A^+_{\leq \theta,\delta} A_{\leq \theta,\delta} Z\rangle| \leq \epsilon$ *in time* $\tilde{O}\left(\left(\kappa(X)\mu(X)\log(1/\varepsilon) + \frac{(\mu(X)+\mu(\dot{X}))}{\delta\theta}\right)\frac{||Z||}{||A^+_{\leq \theta,\delta} A_{\leq \theta,\delta} Z||}\right)$ *and an estimator* $\overline{\|Y\|}$ *with* $|\overline{\|Y\|} - \|Y\|| \leq \eta \|Y\|$ *with an additional* $1/\eta$ *factor.*

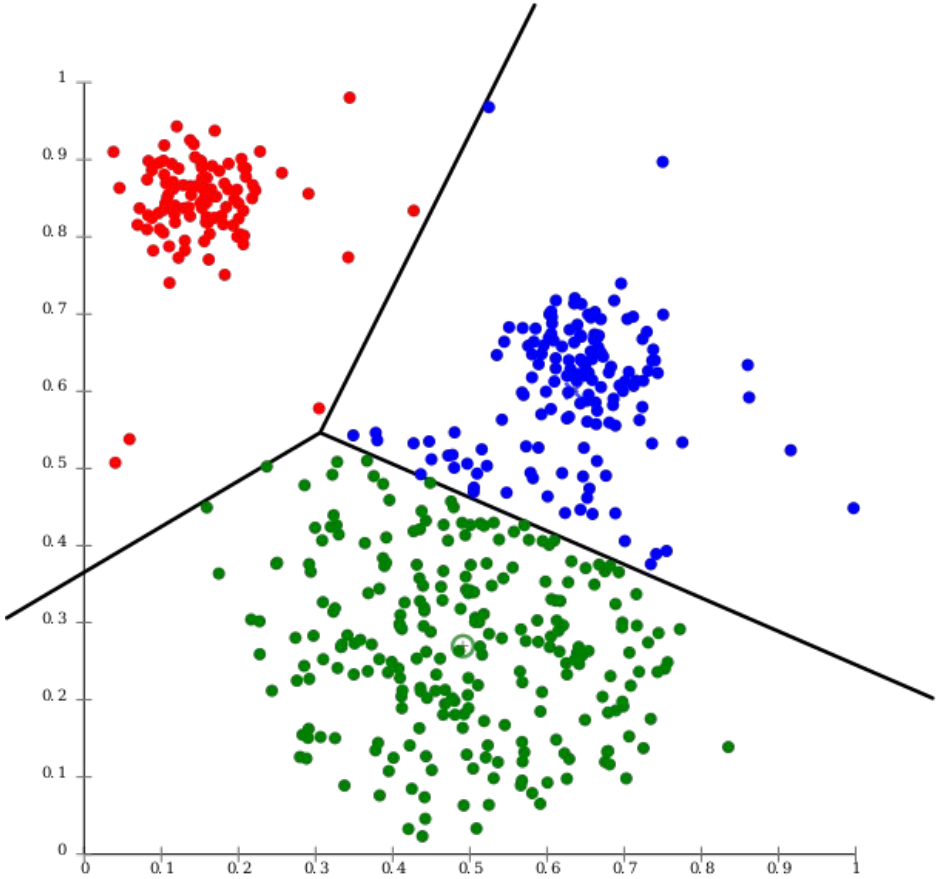


Kerenidis Iordanis, and A. L. "Quantum classification of the MNIST dataset via Slow Feature Analysis." *arXiv preprint arXiv:1805.08837* (2018).

Clustering

Classical algorithm $O(kdn)$

Quantum algorithm $O(kd \log n)$



How big is the market?

High end computing is $5-6bn a year, (IBM) could increase to $10bn.

The size of the market will also **depend on the business model** used (hardware sales vs. cloud-based) (JP Morgan)

return λ

Hacker. Researching in Quantum Machine Learning in academia and in industry. Privacy enthusiast, expertise in cybersecurity. Musician.

- **Blog**
- **Quantum Machine Learning Notes**
- **Cypherpunk**
- **About**
- **Music**

Follow me:

Blog Posts

19 Jul 2018 » Selected articles on Quantum Machine Learning
18 Jul 2018 » Quantum Frobenius Distance Classifier
02 Jul 2018 » Iordanis Kerenidis' talk on quantum machine learning
16 Jun 2018 » Quantum Slow Feature Analysis, a quantum algorithm for dimensionality reduction
10 Jun 2018 » How to evaluate a classifier
15 Apr 2018 » Gather Statistics For Your Qram
15 Apr 2018 » Failed Attempt To Reverse Swap Test
18 Feb 2018 » Hamiltonian Simulation
03 Feb 2018 » Storing Data In A Quantum Computer
29 Jan 2018 » Swap Test For Distances
27 Dec 2017 » Space Estimation Of Hhl
04 Dec 2017 » Rewriting Swap Test
21 Nov 2017 » The Hhl Algorithm
06 Jan 2017 » Transavia is not recommended for travelling musicians
06 Jan 2017 » My i3 configuration for Qubes-OS
21 Aug 2016 » Migrations and functors
13 Jun 2016 » A primer on Projective Simulation: a (quantum) ML algorithm.
11 Apr 2016 » CCNOT on a Feyman's quantum computer
01 Apr 2016 » Palindromic Fibonacci in python
21 Mar 2016 » The twelvefold pythonic way (WIP post)
10 Mar 2016 » When ugly code must be written IRL: i.e. putting password inside the code like a pr0
09 Mar 2016 » Whonix AppVM won't connect to Tor after hybernate
26 Feb 2016 » Some ideas: (part two)

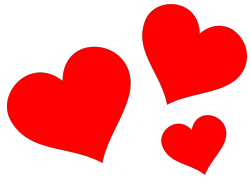
Quantum Finance

- Optimal feature selection for credit scoring
- Optimal trading strategy optimal arbitrage opportunities
- Pricing derivatives
- Risk analysis (VaR, CVar)

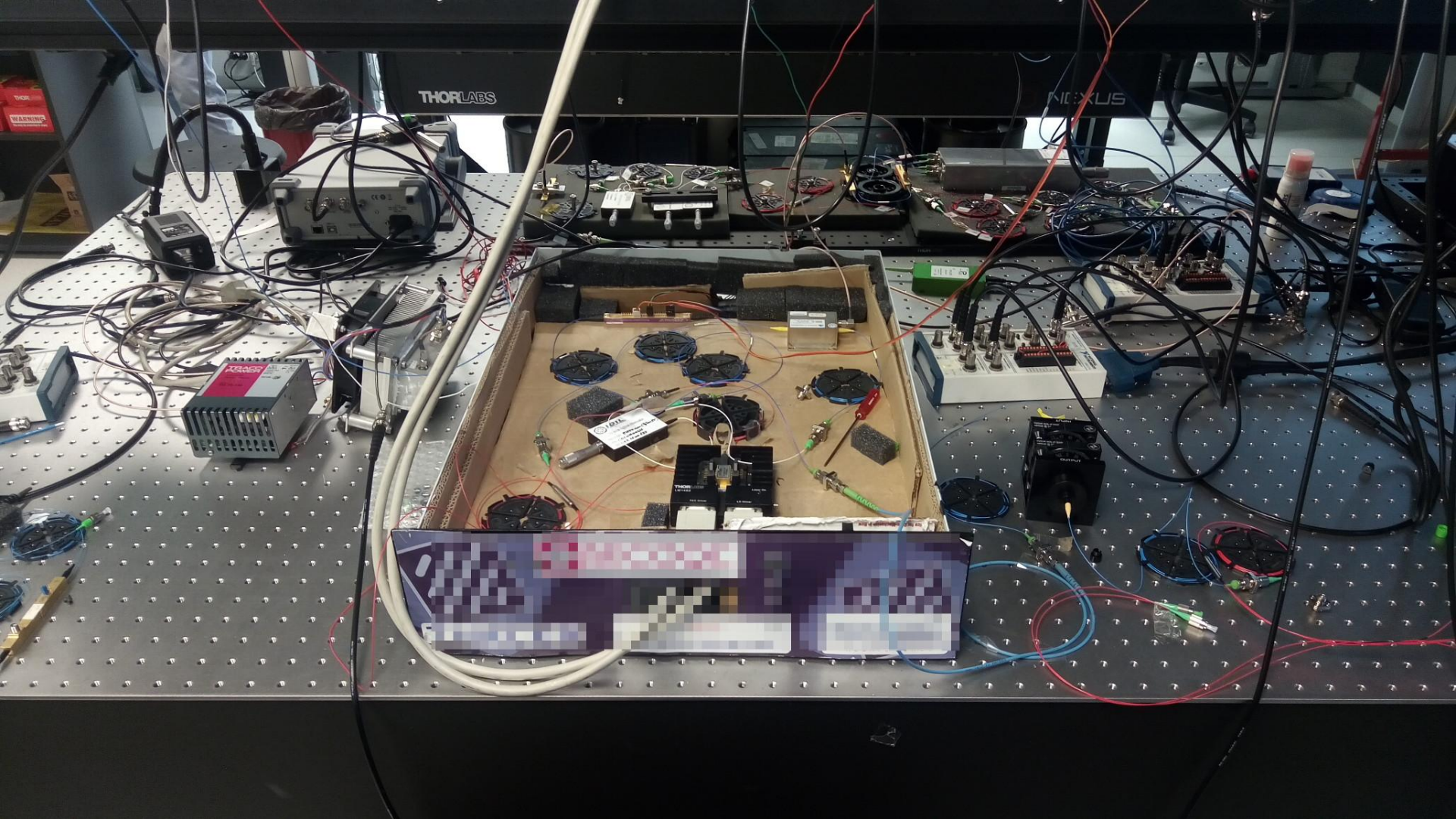
- Quantum computing for finance: overview and prospects. R. Orus, S. Mugel, E. Lizaso https://arxiv.org/abs/1807.03890
- Quantum speedup of Monte Carlo methods. *Proc. R. Soc. A* 471.2181 (2015): 20150301. Montanaro, Ashley.
- Quantum Risk Analysis. - Stefan Woerner, Daniel J. Egger https://arxiv.org/abs/1806.06893

Quantum Communications?

1. BB84 offers **information-theoretical security**
2. **Position based quantum cryptography**
3. **Delegation** of quantum computation
4. Classical **homomorphic encryption** for quantum circuit
5. Quantum links:
   a. LAN: ok
   b. Satellite: medium
   c. Long distance: research needed on repeaters!



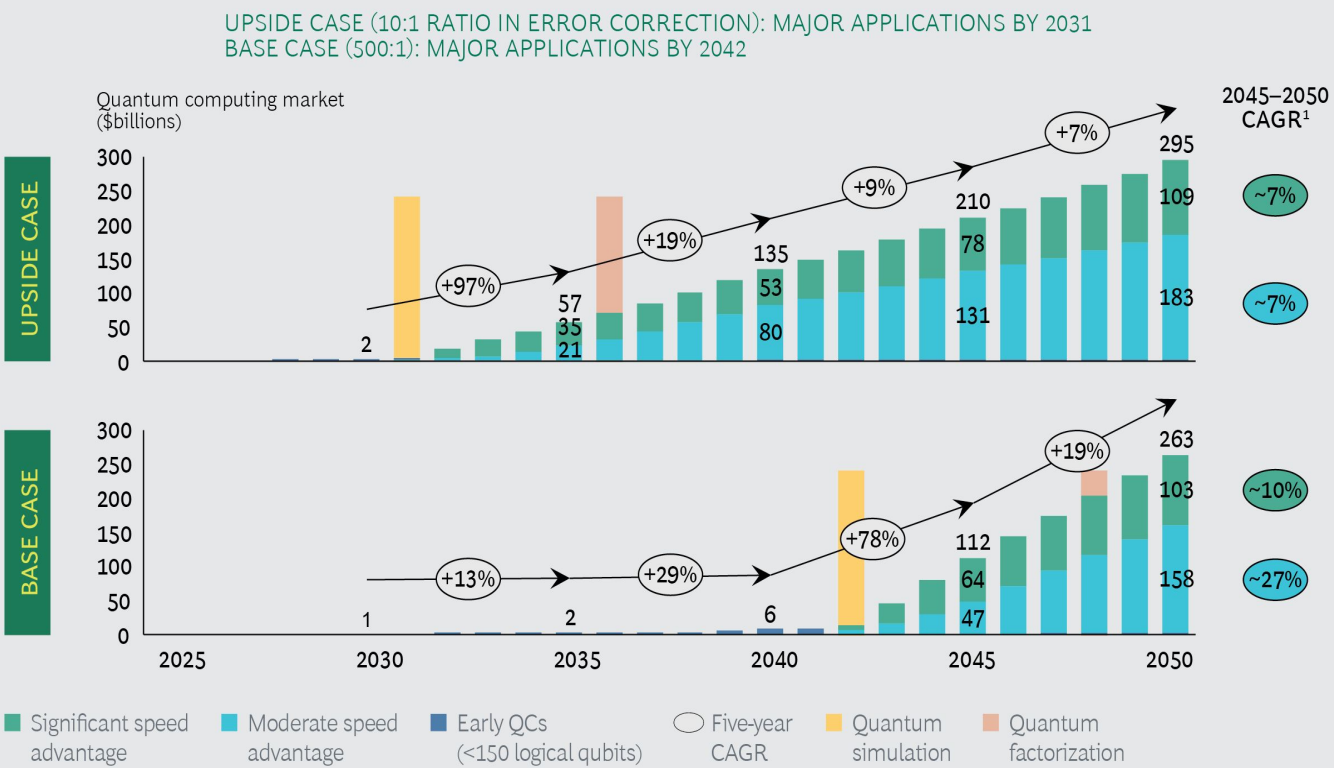
Quantum Crypto will **not** substitute classical cryptography!


THORLABS
WARNING
XP-RACK
XP-RACK

Who's playing?

IBM **Research**

EXHIBIT 3 | The Speed of Market Growth Depends on Technical Milestones



Source: BCG analysis.
Note: Assumes machine learning grows at current projected rate of ~18% CAGR until 2037 and then levels off at 2% CAGR per year until reaching a steady-state growth rate of ~7% applied to majority of other applications. Because of rounding, numbers may not add up to the totals shown.
[1]CAGR based on 2045–2050 to compensate for downward bias of higher initial adoption rates of solutions that offer significant and moderate speed advantages.

Source: BCG Coming quantum computing leap https://www.bcg.com/publications/2018/coming-quantum-leap-computing.aspx

So what?

- Gap between theory and technology to fill.
  - **New kind of information to process!**
  - We should program and test q-algorithms and fine-tune them
  - **Find new domains** where quantum can be applied (nuclear reactors, but also 5G technology, medicine,)
  - Still waiting for **quantum advantage…**
  - **> 2.5 billions** of public funding in next years

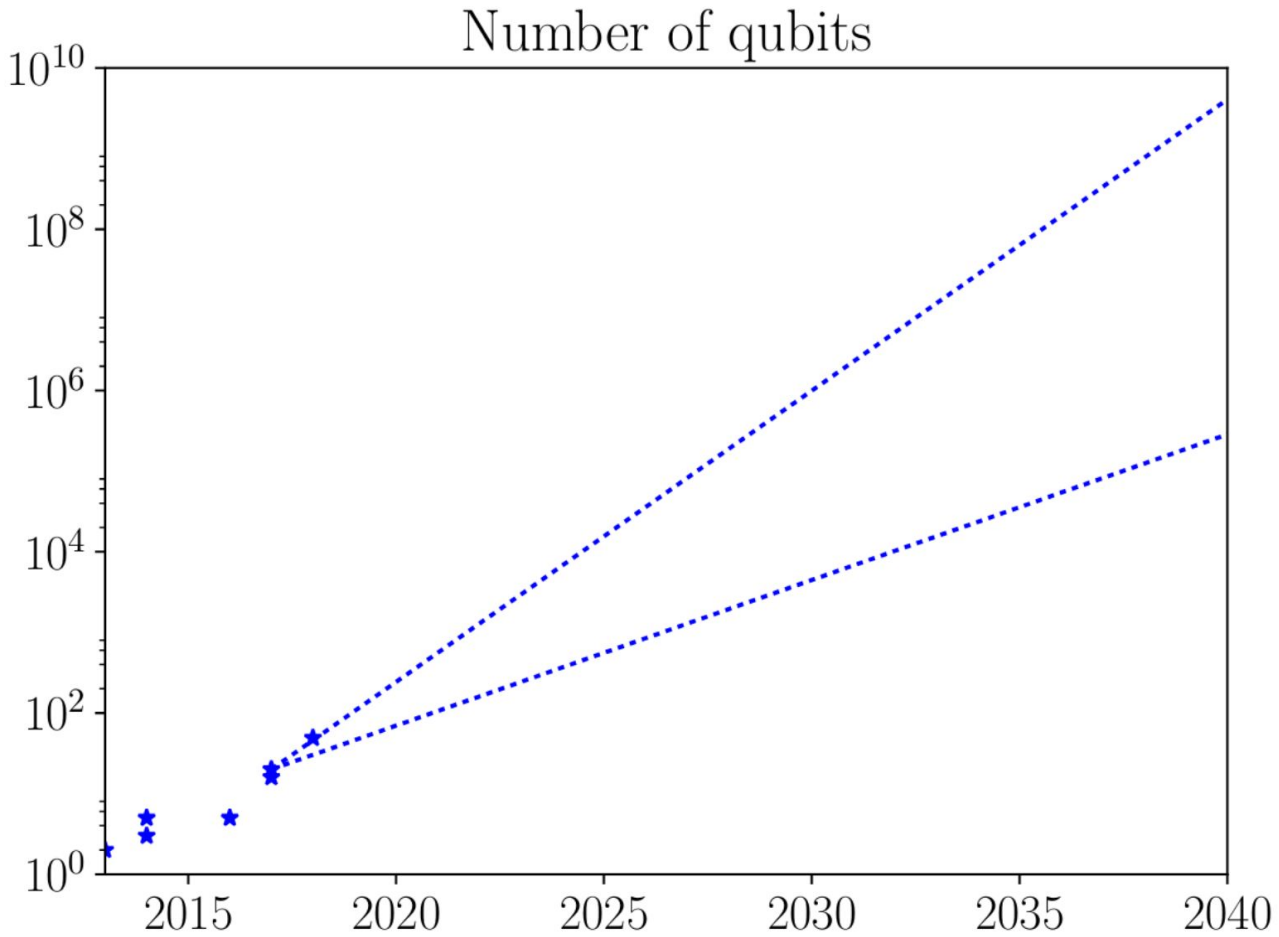
So what?

- Find business models:
  - **Train** and give the model to customers?
  - **Consulting**?
  - Will be a **platform as a service**?
- Write and test code
  - The software stack! (we are still doing arithmetics!)
  - The **glue** to use the software
  - Learn how to do **data analytics** on quantum computer!

Get in touch if your company wants to know more about quantum algorithms or you have a problem to solve.

Thanks for your time,
there's never enough.

cit. Dan Geer



Aggarwal, Divesh, et al. "Quantum attacks on Bitcoin, and how to protect against them." *arXiv preprint arXiv:1710.10377* (2017).

Organization	Adiabatic	Superconducting	Trapped Ion	Neutral Atom	Spin/Quantum Dot	Photonic	NV Diamond	Topological
Alpine Quantum Technologies			X					
Atom Computing				X				
Bleximo		X						
CEA-Leti / Inac					X			
Centre for Quantum Computation & Communication Technology					X	X		
Chalmers University of Technology		X						X
Duke University			X			X		
D-Wave	X							
Google	X	X						
Griffith Univ./Univ. Of Queensland						X		
Honeywell			X					
IBM		X						
ID Quantique						X		
Institut d'Optique				X				
Intel		X			X			
IonQ			X					
IQM Finland		X						
Microsoft								X
MIT Lincoln Lab	X	X	X				X	
MIT/Univ. of Innsbruck			X					
Niels Bohr Institute								X
Nokia Bell Labs								X
NQIT			X					
NTT/Japan NII/Univ. of Tokyo						X		
Oxford		X	X			X	X	
Oxford Quantum Circuits		X						
Penn State University				X				
PsiQuantum						X		
Qilimanjaro	X							
Quantic		X						
Quantum Circuits Inc		X						
Quantum Factory			X					
Qubitekk						X		
QuTech		X			X		X	X
Rigetti		X						
Sandia National Laboratories			X	X	X			
SeQureNet						X		
Simon Fraser University					X			
Sparrow Quantum						X		
Toshiba						X		
TundraSystems Global						X		
Turing								
TU Wein/NII Tokyo/NTT								
Universitat Duisburg-Essen								
University of Bristol								
University of California Santa Barbara								
Joint Quantum Institute / University of Maryland								
University. of Science & Technology of China (USTC)								
University of Basel								
University of Sussex								
University of Washington								
University of Waterloo - IQC								
University of Wisconsin								
Weizmann Institute								
Xanadu								
Yale Quantum Institute								

From: Quantum Computing Report:
https://quantumcomputingreport.com/