

AI CENTER
FEE CTU

Quantum Computing

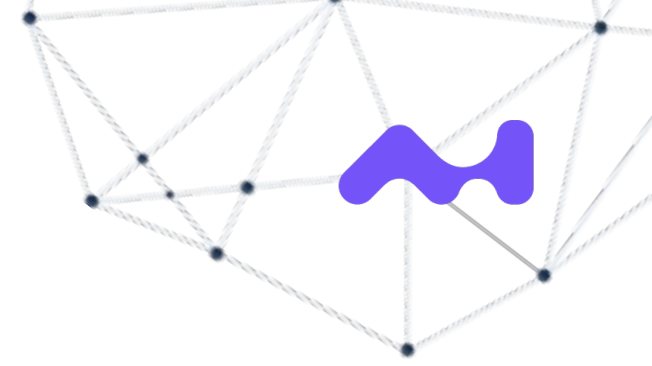
Johannes Aspman, Georgios Korpas, Jakub Mareček, Germán Matilla

Faculty of Electrical Engineering
Czech Technical University in Prague

February 24th, 2023

Quantum Computing

1. Motivation: "A social phenomenon"
2. Motivation: Opportunities and Limitations
3. Organization of the Course
4. Qubits and How to Implement them
5. A Theoretical Computer Science point of view
6. Three use cases in financial services

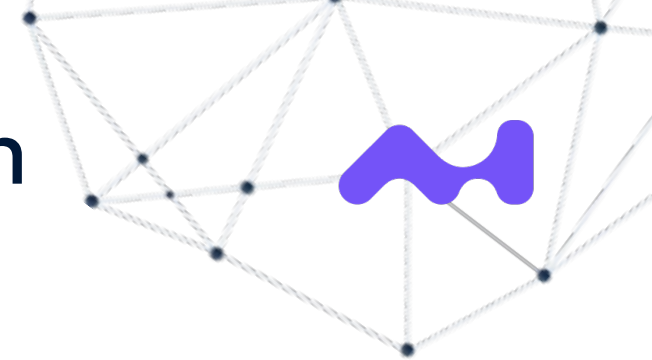


Quantum Computing: A Short History



- 1965: Nobel prize for Richard P. Feynman.
- 1973: Alexander Holevo publishes a paper showing that n qubits can carry more than n classical bits of information, but at most n classical bits are accessible.
- 1973: Charles H. Bennett publishes papers on reversible computing.
- 1980: Tommaso Toffoli introduces the Toffoli gate, which is a key element in both classical reversible computing and quantum computing.
- 1980: Paul Benioff and Yuri Manin publish papers on quantum computing.
- 1981: At the "First Conference on the Physics of Computation," Paul Benioff and Richard Feynman give talks on quantum computing.
- 1985: David Deutsch introduces the first universal model of quantum computing.
- 1993: Dan Simon suggests the so-called Simon's problem, for which a quantum computer could be exponentially faster than a conventional computer (under mild assumptions on the oracles).
- 1994: Peter Shor extends Simon's work to Shor's algorithm for factoring integers.
- 1998: A team incl. Isaac L. Chuang demonstrates a 2-qubit NMR-based quantum computer.
- 2022: Nobel prize for Alain Aspect, John F. Clauser and Anton Zeilinger.

Quantum Computing: A Social Phenomenon



- Feynman (1986): "Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy." ("Proof by authority")
- A prototypical problem: Computing the ground-state energy (eigenvalue of the fermionic Hamiltonian), usually discretized into a basis (of size L). One needs to restrict oneself to "generic" molecules and materials.
- Seth Lloyd (1996): Exponential quantum advantage conjecture
- Kitaev (2003): Ground state characterization is QMA (cf. the Ising Hamiltonian)

<https://www.ams.org/books/gsm/047/>

<https://www.science.org/doi/abs/10.1126/science.273.5278.1073>

<https://arxiv.org/abs/quant-ph/0302079> <https://arxiv.org/abs/quant-ph/0406180v2>

<https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.3.010318>

<https://simons.berkeley.edu/events/quantum-colloquium-there-evidence-exponential-quantum-advantage-quantum-chemistry>

RESEARCH ARTICLES

Universal Quantum Simulators

Seth Lloyd

Feynman's 1982 conjecture, that quantum computers can be programmed to simulate any local quantum system, is shown to be correct.

Over the past half century, the logical devices by which computers store and process information have shrunk by a factor of 2 every 2 years. A quantum computer is the end point of this process of miniaturization—when devices become sufficiently small, their behavior is governed by quantum mechanics. Information in conventional digital computers is stored on capacitors. An uncharged capacitor registers a 0 and a charged capacitor registers a 1. Information in a quantum computer is stored on individual spins, photons, or atoms. An atom can itself be thought of as a tiny capacitor. An atom in its ground state is analogous to an uncharged capacitor and can be taken to register a 0, whereas an atom in an excited state is analogous to a charged capacitor and can be taken to register a 1.

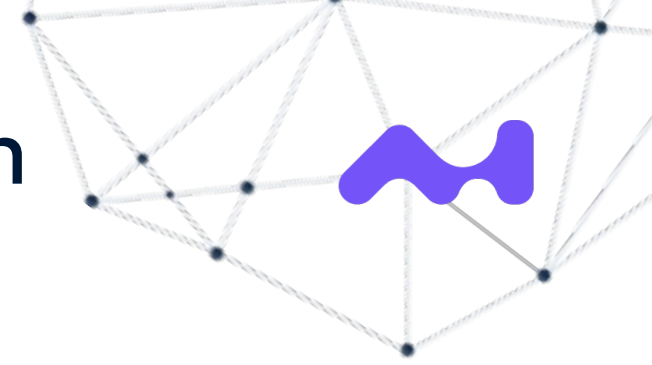
So far, quantum computers sound very much like classical computers; the only use of quantum mechanics has been to make a correspondence between the discrete quantum states of spins, photons, or atoms and the discrete logical states of a digital computer. Quantum systems, however, exhibit behavior that has no classical analog. In particular, unlike classical systems, quantum systems can exist in superpositions of different discrete states. An ordinary capacitor can be either charged or uncharged, but not both: A classical bit is either 0 or 1. In contrast, an atom in a quantum superposition of its ground and excited state is a quantum bit that in some sense registers both 0 and 1 at the same time. As a result, quantum computers can do things that classical computers cannot.

Classical computers solve problems by using nonlinear devices such as transistors to perform elementary logical operations on bits. Over the past 50 years, a considerable amount of effort has been devoted to such simulation. Much information about a quantum system's dynamics can be extracted from semiclassical approximations (when classical solutions are known), and ground state properties and correlation functions

can be extracted with Monte Carlo methods (30–32). Such methods use amounts of computer time and memory space that grow as polynomial functions of the size of the quantum system of interest (where size is measured by the number of variables—particles or lattice sites, for example—required to characterize the system). Problems that can be solved by methods that use polynomial amounts of computational resources are commonly called tractable; problems that can only be solved by methods that use exponential amounts of resources are commonly called intractable. Feynman pointed out that the problem of simulating the full time evolution of arbitrary quantum systems on a classical computer is intractable: The states of a quantum system are wave functions that lie in a vector space whose dimension grows exponentially with the size of the system. As a result, it is an exponentially difficult problem merely to record the state of a quantum system, let alone integrate its equations of motion. For example, to record the state of 40 spin-1/2 particles in a classical computer's memory requires $2^{40} \approx 10^{12}$ numbers, whereas to calculate their time evolution requires the exponentiation of a $2^{40} \times 2^{40}$ matrix with $\sim 10^{16}$ entries. Feynman asked whether it might be possible to bypass this exponential explosion by having one quantum system simulate another directly, so that the states of the simulator obey the same equations of motion as the states of the simulated system. Feynman gave simple examples of one quantum system simulating another and conjectured that there existed a class of universal quantum simulators capable of simulating any quantum system that evolved according to local interactions.

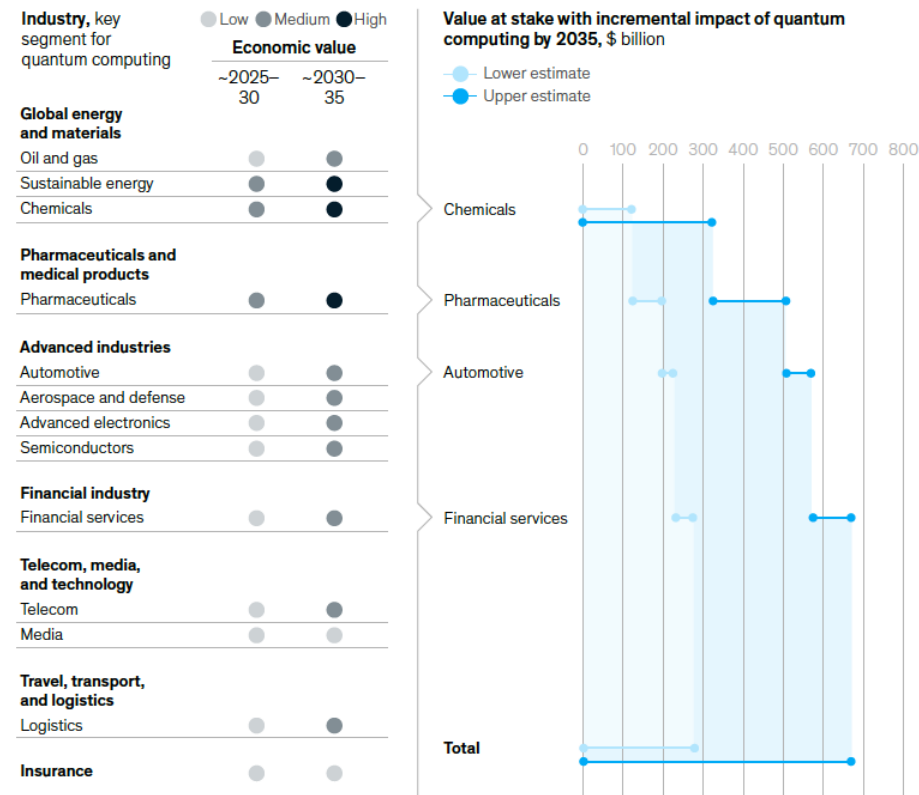
The answer to Feynman's question is, yes. I will show that a variety of quantum systems, including quantum computers, can be "programmed" to simulate the behavior of arbitrary quantum systems whose dynamics are determined by local interactions. The programming is accomplished by inducing the interactions between the variables of the simulator that initiate the interactions between the variables of the system to be simulated; in other words, the dynamics of the properly programmed simulator and the dynamics of the system to be simulated are one and the same to within any desired accuracy. So, to simulate the time evolution of 40 spin-1/2 particles over time t requires a simulator with 40 quantum bits evolving

Quantum Computing: A Social Phenomenon



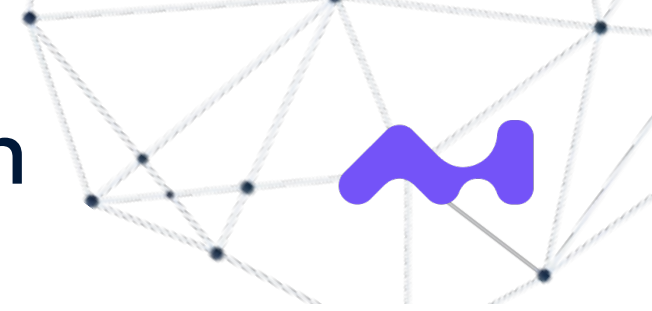
- McKinsey recommendations to CEOs (December 2021):

Conservatively, we estimate that the value at stake in pharmaceuticals, chemicals, automotive, and finance use cases could be up to nearly \$700 billion.



1. Follow industry developments and actively screen quantum-computing use cases with an in-house team of quantum-computing experts or by collaborating with industry entities and by joining a quantum-computing consortium.
2. Understand the most significant risks and disruptions and opportunities in their industries.
3. Consider whether to partner with or invest in quantum-computing players—mostly software—to facilitate access to knowledge and talent.
4. Consider recruiting in-house quantum-computing talent. Even a small team of up to three experts may be enough to help an organization explore possible use cases and screen potential strategic investments in quantum computing.
5. Prepare by building digital infrastructure that can meet the basic operating demands of quantum computing; make relevant data available in digital databases and set up conventional computing workflows to be quantum ready once more powerful quantum hardware becomes available.

Quantum Computing: A Social Phenomenon



American Banker:

- 25% of financial institutions already invest in quantum
- 45% plan to invest in 2023

Gartner:

- 40% of large companies are planning to create initiatives around quantum computing by 2025.

AMERICAN BANKER

BANKING ▾ POLICY ▾ PAYMENTS ▾ TECH ▾ CREDIT UNIONS ▾ WORKPLACE ▾ OPINION

Find your interest!

TECHNOLOGY

How JPMorgan Chase and other banks plan to use quantum computing

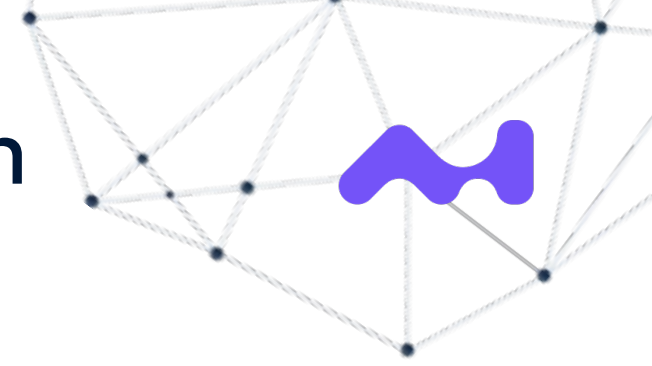
By [Penny Crosman](#) September 22, 2022, 2:57 p.m. EDT 5 Min Read



Though quantum computing technology is still new, JPMorgan Chase, Ally Bank, Credit Agricole and other banks are actively testing and in some cases using it, according to speakers at the HPC + AI on Wall Street conference in New York this week.

"We realize that if a company doesn't do anything about the market right now, and just waits for quantum advantage to become a reality, when quantum advantage becomes real, it might be too late," said Marco Pistoia, managing director, distinguished engineer, head of global technology applied research and head of quantum computing at JPMorgan Chase. "We want to be ready when quantum advantage becomes possible on a higher level."

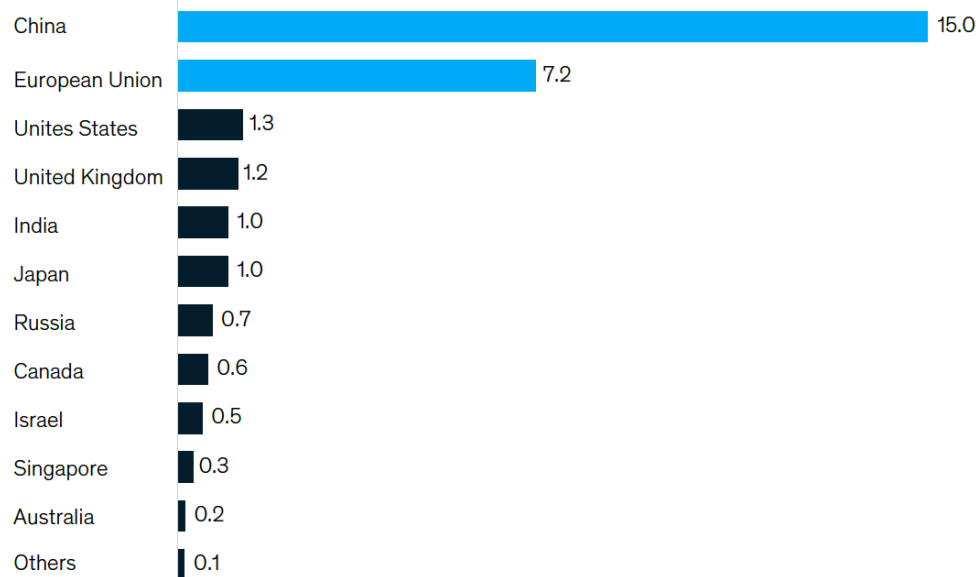
Quantum Computing: A Social Phenomenon



- Circa \$80B eco-system
- \$20+B of public funding announced
- \$1.7B private investment in 2021

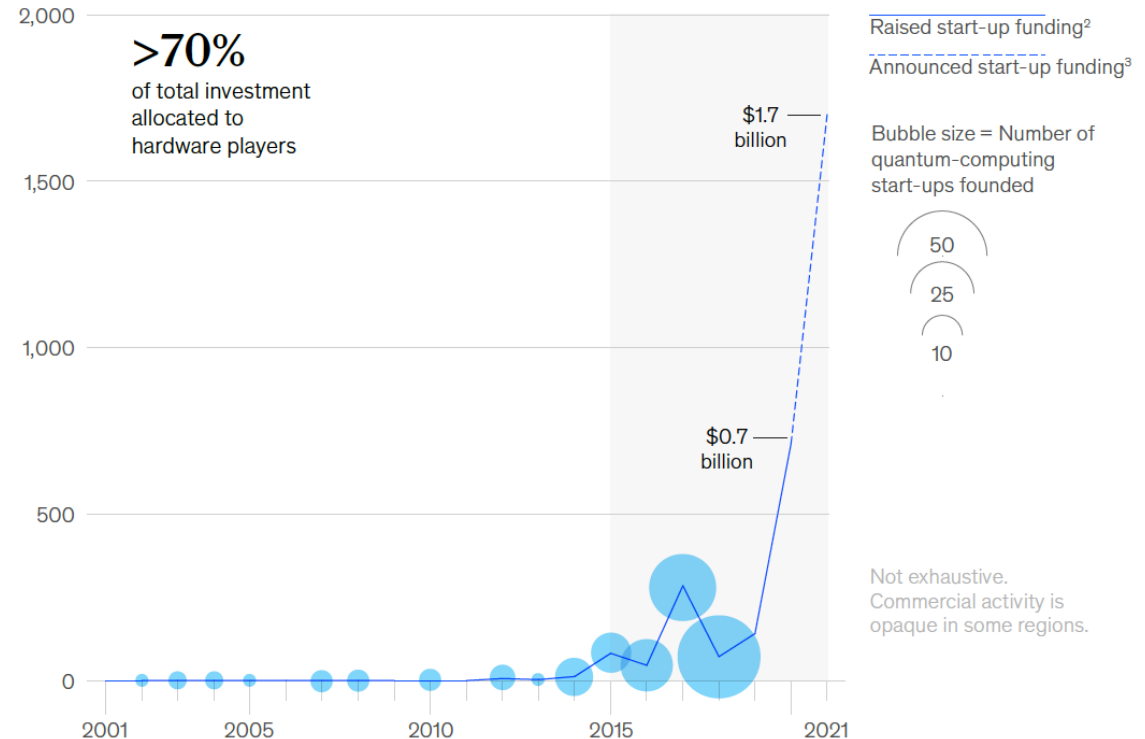
China and the European Union lead significantly on public funding for quantum computing.

Announced planned governmental funding,¹\$ billions



Start-up activity and investments in quantum computing have skyrocketed since 2015.

Volume¹ of raised funding, \$ millions



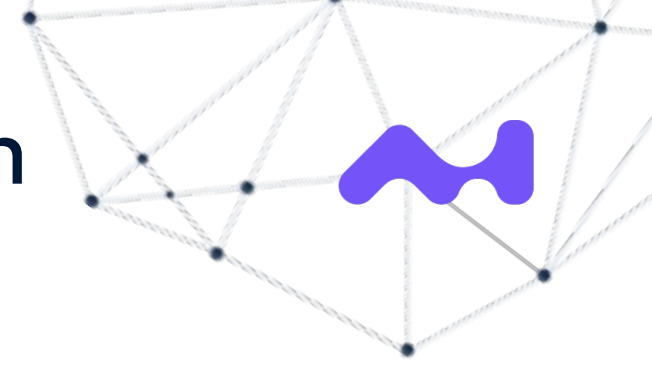
¹Based on public investment data recorded in PitchBook; actual investment is likely higher.

²Public announcements of major deals; actual investment is likely higher.

³Start-ups from 2019 and later are likely still in stealth mode or are not yet recognized as quantum-computing companies by relevant platforms and experts.

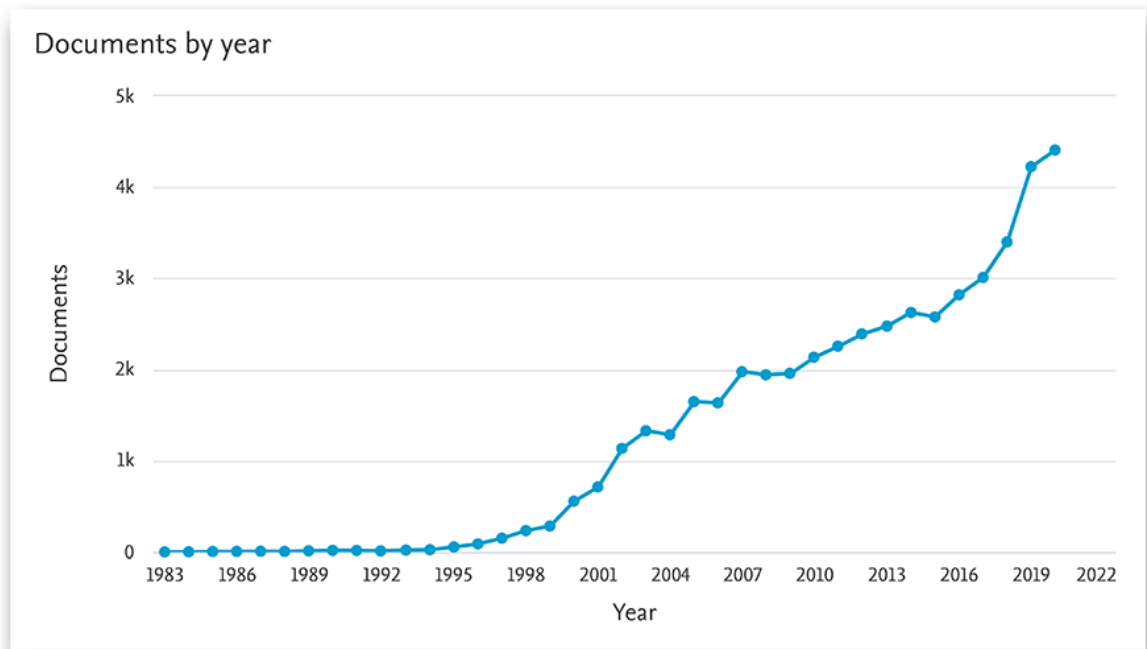
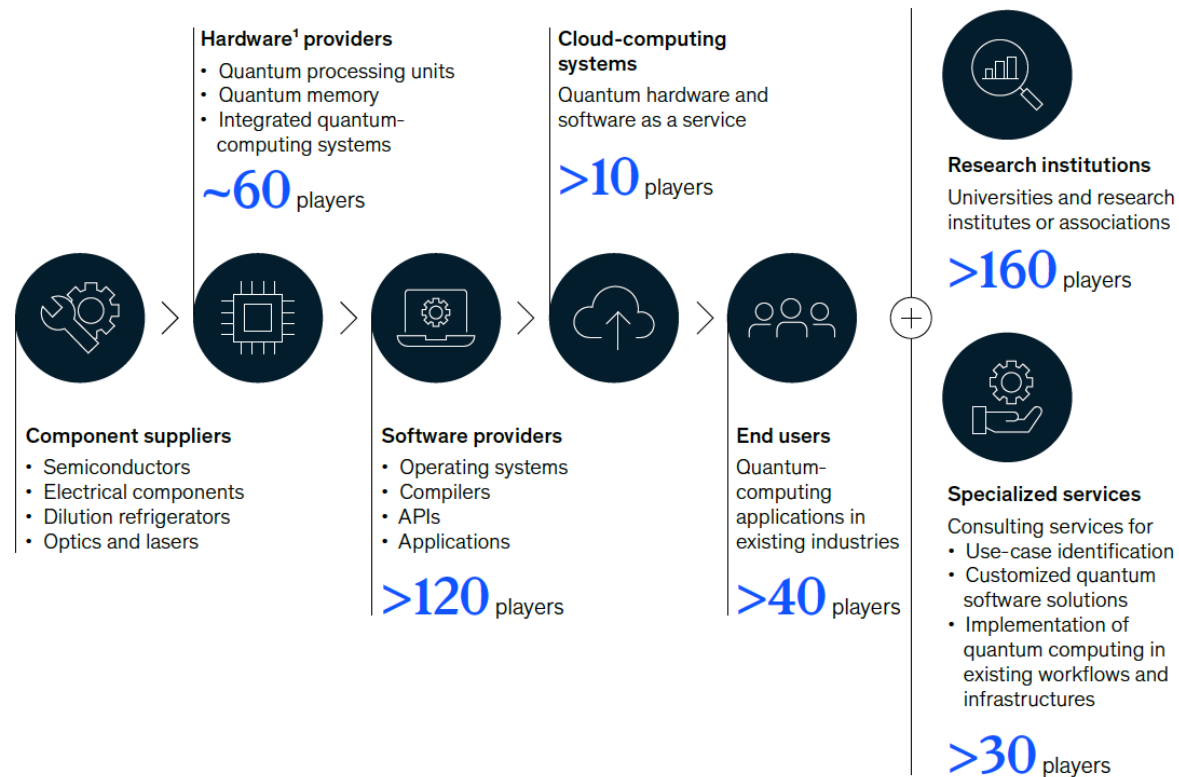
Source: PitchBook; McKinsey analysis

Quantum Computing: A Social Phenomenon



In the quantum-computing value chain, software has the largest number of players.

Overview of players in the quantum-computing value chain



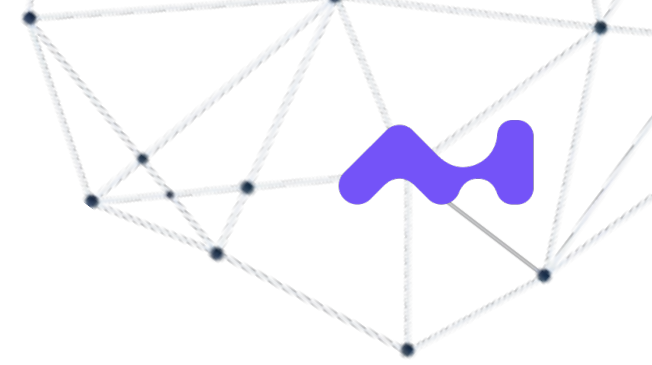
Opportunities

Seen by John Preskill:

- There are problems that are **believed** to be hard for classical computers, but for which quantum algorithms have been discovered that could solve these problems easily under mild assumptions. E.g. factoring.
- Measuring qubits in certain states, which are easy to prepare, samples from a correlated probability distribution that can't be sampled from by any efficient classical means (unless the polynomial hierarchy collapses).
- No known classical algorithm can simulate a quantum computer efficiently.

Seen by yours truly:

- Quantum computers are essentially analog computers, cf. "complexity over the reals", which may violate the "Extended Church-Turing Thesis".
- We seem to have



Article | [Published: 23 October 2019](#)

Quantum supremacy using a programmable superconducting processor

[Frank Arute](#), [Kunal Arya](#), [Ryan Babbush](#), [Dave Bacon](#), [Joseph C. Bardin](#), [Rami Barends](#), [Rupak Biswas](#), [Sergio Boixo](#), [Fernando G. S. L. Brandao](#), [David A. Buell](#), [Brian Burkett](#), [Yu Chen](#), [Zijun Chen](#), [Ben Chiaro](#), [Roberto Collins](#), [William Courtney](#), [Andrew Dunsworth](#), [Edward Farhi](#), [Brooks Foxen](#), [Austin Fowler](#), [Craig Gidney](#), [Marissa Giustina](#), [Rob Graff](#), [Keith Guerin](#), ... [John M. Martinis](#)  [+ Show authors](#)

[Nature](#) 574, 505–510 (2019) | [Cite this article](#)

Quantum computational advantage using photons

[HAN-SEN ZHONG](#) , [HUI WANG](#) , [YU-HAO DENG](#) , [MING-CHENG CHEN](#) , [LI-CHAO PENG](#) , [YI-HAN LUO](#) , [JIAN QIN](#) , [DIAN WU](#) , [XING DING](#) , [...]

AND [JIAN-WEI PAN](#)  [+14 authors](#) [Authors Info & Affiliations](#)

[SCIENCE](#) · 3 Dec 2020 · Vol 370, Issue 6523 · pp. 1460-1463 · [DOI: 10.1126/science.abe8770](#)

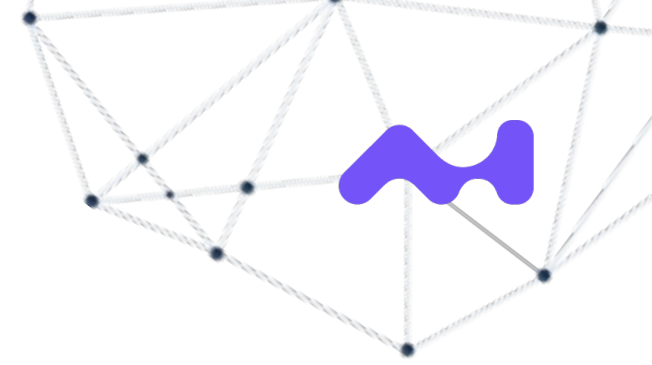
Article | [Open Access](#) | [Published: 22 February 2023](#)

Suppressing quantum errors by scaling a surface code logical qubit

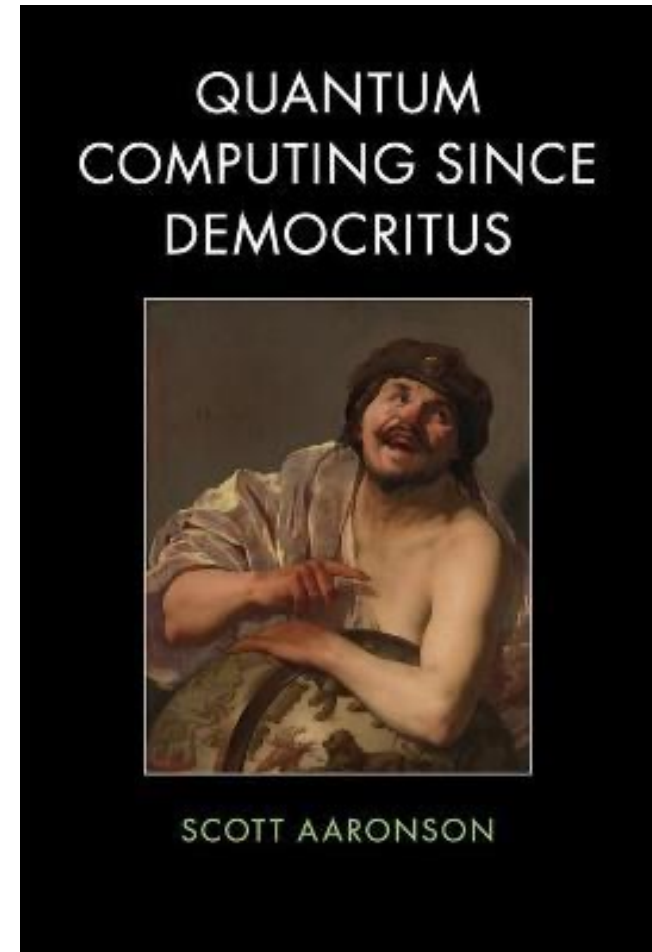
[Google Quantum AI](#)

[Nature](#) 614, 676–681 (2023) | [Cite this article](#)

Eleven Objections of Scott Aaronson



- Works on paper, not in practice.
- Violates Extended Church-Turing Thesis.
- Not enough "real physics."
- Small amplitudes are unphysical.
- Exponentially large states are unphysical.
- Quantum computers are just souped-up analog computers.
- Quantum computers aren't like anything we've ever seen before.
- Quantum mechanics is just an approximation to some deeper theory.
- Decoherence will always be worse than the fault-tolerance threshold.
- We don't need fault-tolerance for classical computers.
- Errors aren't independent.



Quantum Computing

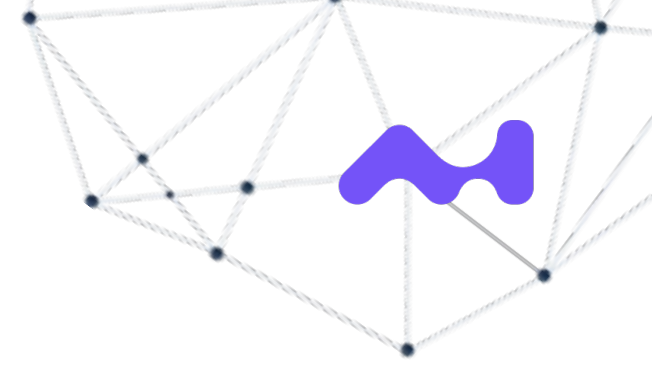
1. Motivation: "A social phenomenon"
2. Motivation: Opportunities and Limitations
3. Organization of the Course
4. Qubits and How to Implement them
5. A Theoretical Computer Science point of view
6. Three use cases in financial services



Course Organization: The Team

Who is involved?

- Bengt Arne **Johannes** Hansson Aspman
- **Georgios** Korpas
- **Jakub** Mareček
- **Germán** Martínez Matilla



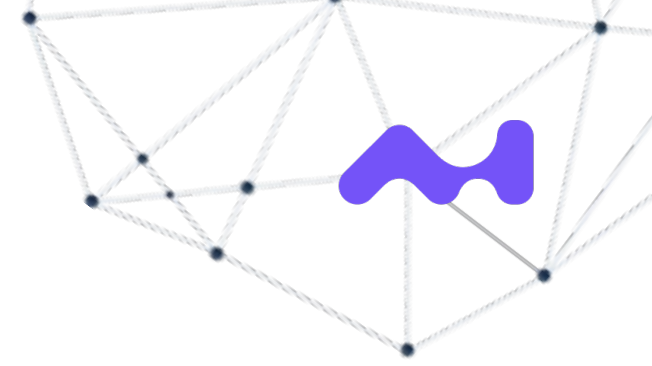
Course Organization: Syllabus

- 1. Why quantum computing? What is quantum computation good for? The notions of quantum supremacy and quantum advantage. Has Google showcased the former? Why studying quantum computation can also push the limits of classical computation by finding better algorithms or quantum inspired algorithms. The global quantum computing scene. **(Jakub and Georgios)**
- 2. Broad picture of quantum mechanics. Postulates of quantum mechanics and bra-ket notation. Unitary operators and expectation values. Evolution of quantum states. Classical to quantum bits. The Bloch sphere. Reversible operations on qubits and quantum circuits. State preparation and measurement in quantum mechanics. **(Johannes)**
- 3. Broad overview of computational complexity. Classical Turing machines. The classes P, NP, P-space, Exp. The quantum Turing machine. The classes BQP and QMA. What lies beyond. **(Jakub)**
- 4. Broad overview of classical versus quantum algorithms. Showcase of the exponential speedup of quantum computers using the Deutsch-Josza algorithm. Shor's algorithm, quantum Fourier transform. **(Jakub and Johannes)**
- 5. Grover's algorithm and exponential-time dynamic programming. **(Jakub)**
- 6. Quantum algorithms and quantum random walks. Classical Monte-Carlo and quantum replacements for Monte-Carlo. Applications in Financial Services. **(Georgios)**
- 7. A broad overview of further trends in quantum technologies. Adiabatic computing. Phase estimation. Quantum annealing. Variational algorithms. Quantum Machine Learning. **(Georgios and Jakub)**

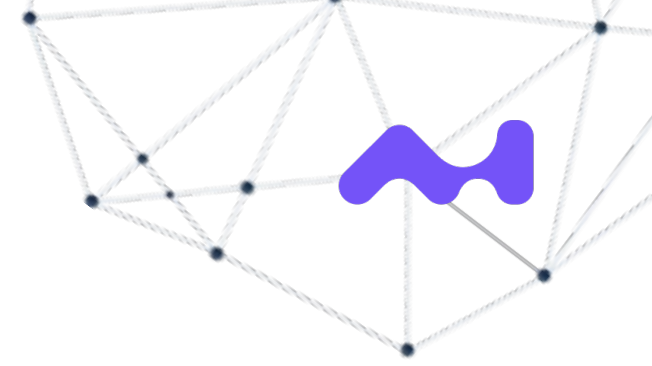


Course Organization: Assessment

- There are 100 points to be collected, which are mapped to grades in the usual fashion (<50 = F, 50-59 = E, ..., 90-100 = A).
- Up to 60 points to be collected during term time (homework and a larger, independent "project").
- To obtain "zapocet", you need to collect at least 30 points during the term time and attend the exercises.
- Up to 40 points are to be collected in a final exam, which can be retaken more than once, if needed.



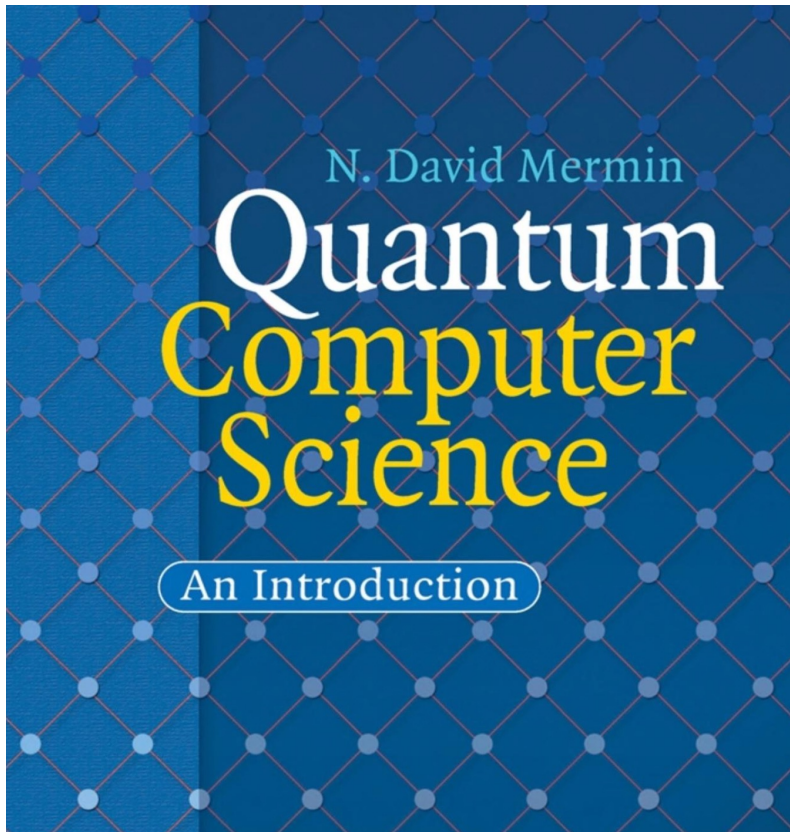
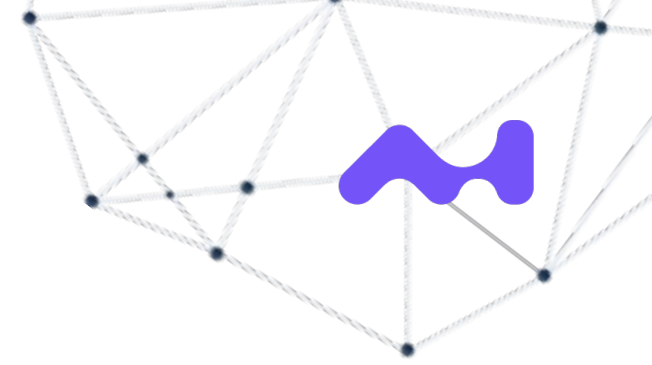
Course Organization: Resources



Lecture notes:

- Focus on contrasting “classical” and “quantum” approaches
- Available before the lecture on-line.
- Is there an interest in hardcopy?

Course Organization: Recommended Text



Miss the old version of the textbook? Access it [here](#)

Qiskit Textbook (beta)

Browse all content

Courses

Basics of quantum information

Single systems

Multiple systems

Quantum circuits

Entanglement in action

Introduction Course

Why Quantum Computing?

The Atoms of Computation

What is Quantum?

Describing Quantum Computers

Entangled States

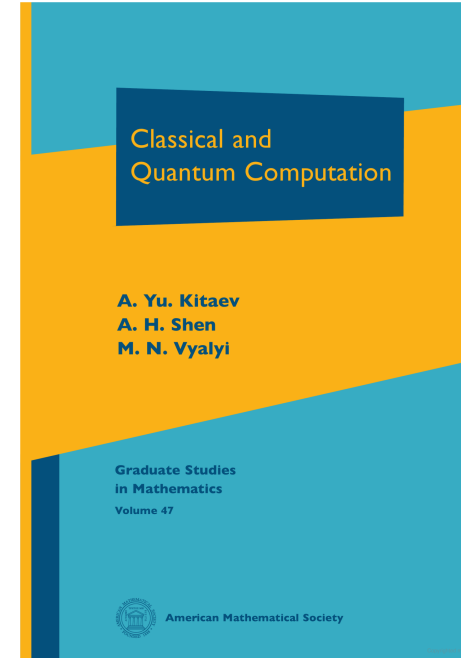
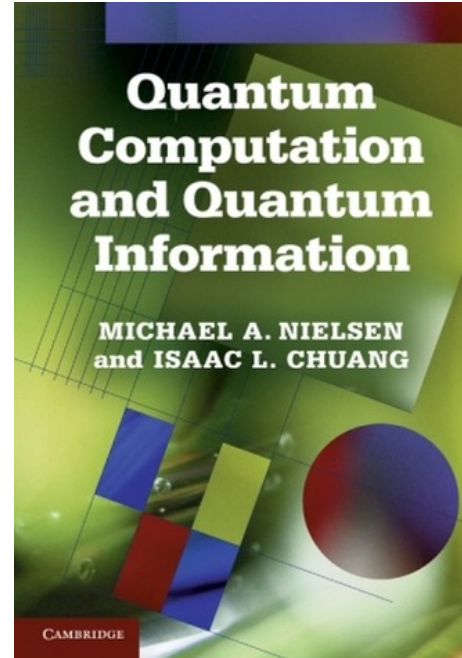
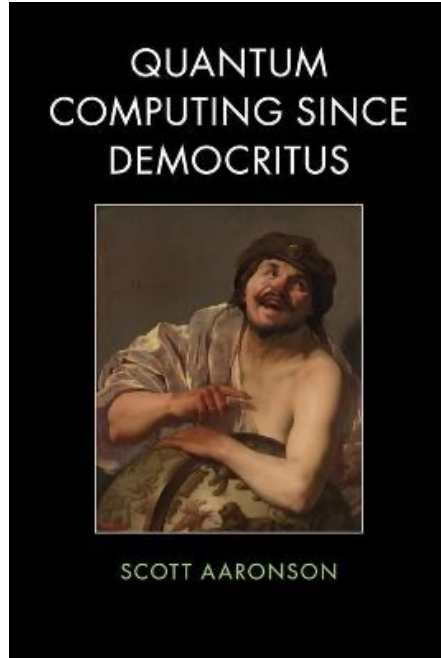
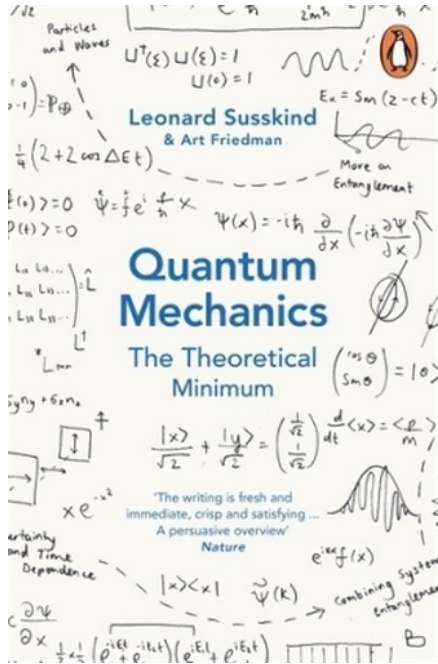
Visualizing Entanglement

Grover's search algorithm

Project

<https://qiskit.org/learn/>

Course Organization: Further Reading



244 Kc at Megabooks <https://www.scottaaronson.com/democritus/>

<https://www.ams.org/books/gsm/047/>

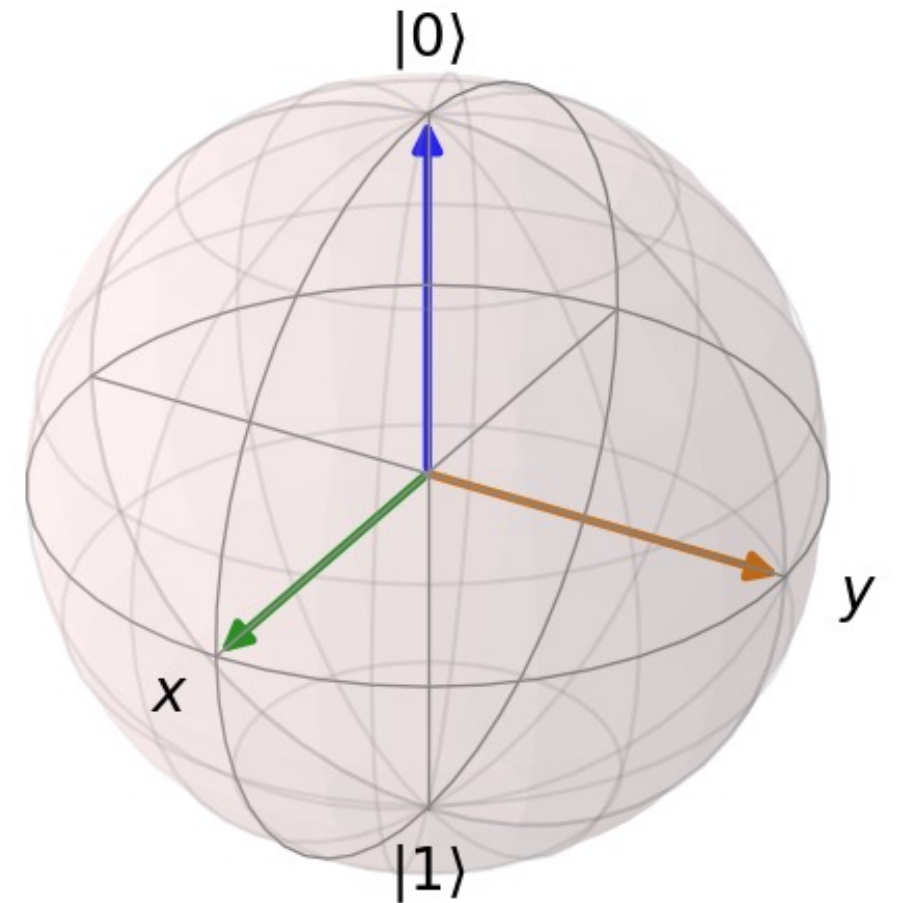
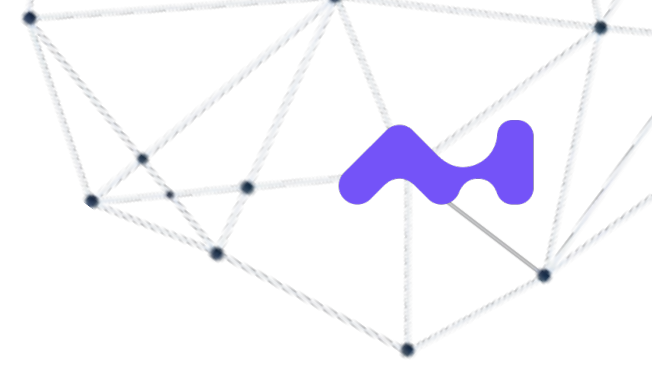
Quantum Computing

1. Motivation: "A social phenomenon"
2. Motivation: Opportunities and Limitations
3. Organization of the Course
4. Qubits and How to Implement them
5. A Theoretical Computer Science point of view
6. Three use cases in financial services

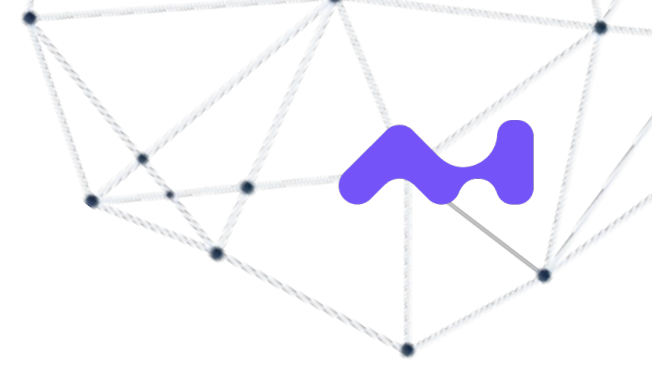


Qubits and How to Implement Them

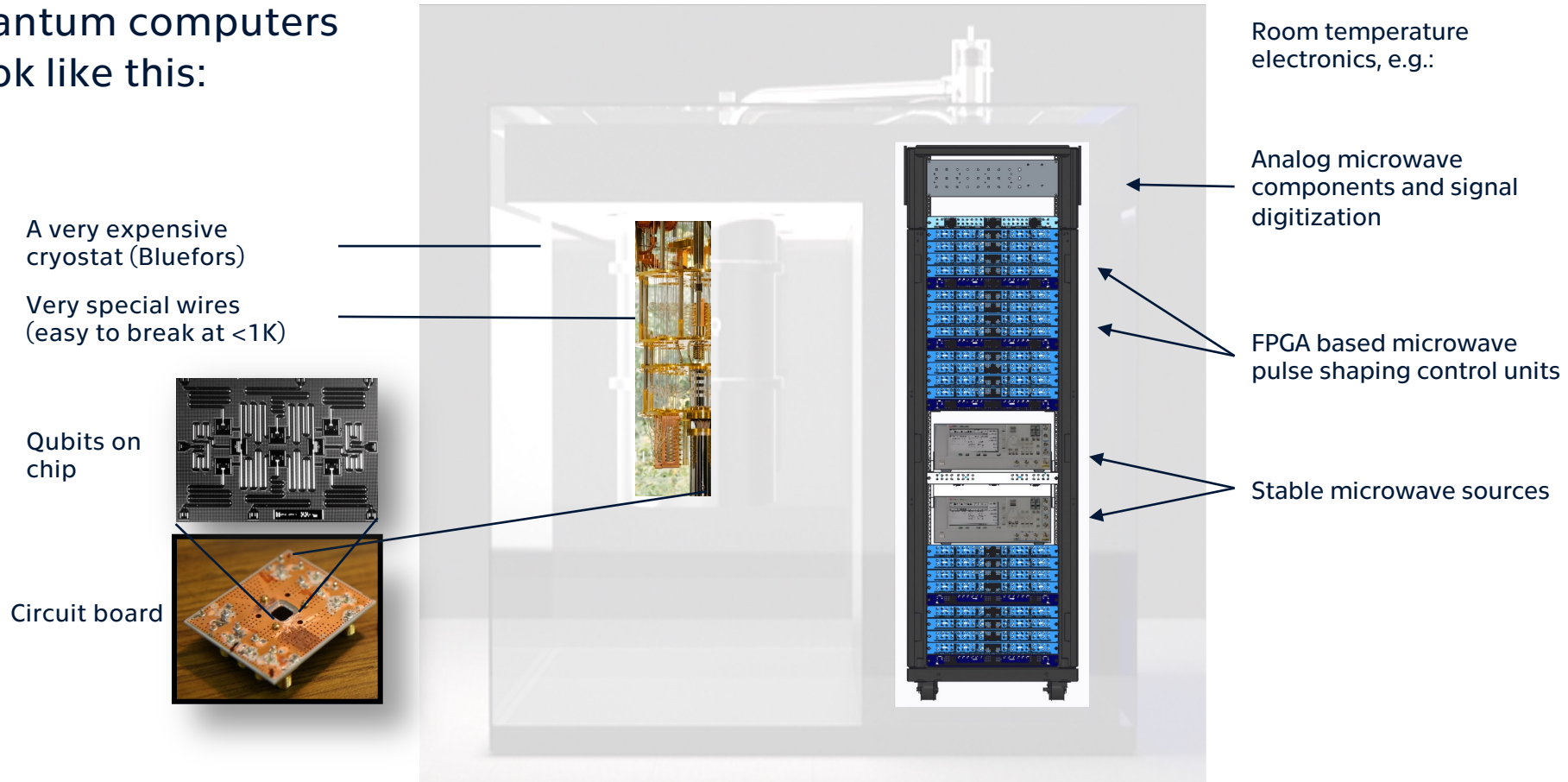
- Digital computers vs. “analog computers”
- $\{0, 1\}$ vs. the state vector $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ of 2 complex numbers α, β
- Bloch-sphere representation thereof
- n qubits, 2^n complex numbers



Qubits and How to Implement Them



- Most quantum computers so far look like this:



Are we There yet?

DiVincenzo's criteria:

- A scalable physical system with well-characterized qubit
- The ability to initialize the state of the qubits to a simple fiducial state
- Long relevant decoherence times
- A "universal" set of quantum gates
- A qubit-specific measurement capability

Fortschr. Phys. **48** (2000) 9–11, 771–783

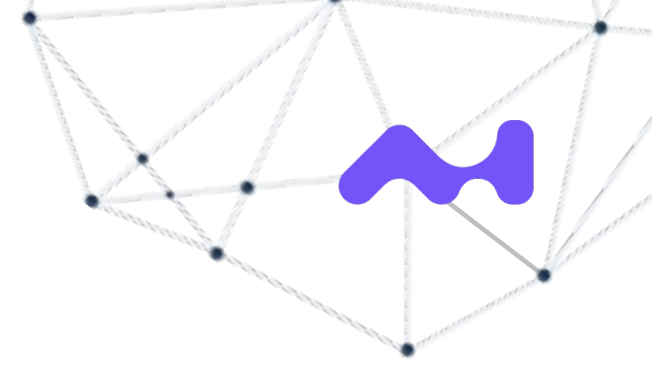
The Physical Implementation of Quantum Computation

DAVID P. DIVINCENZO

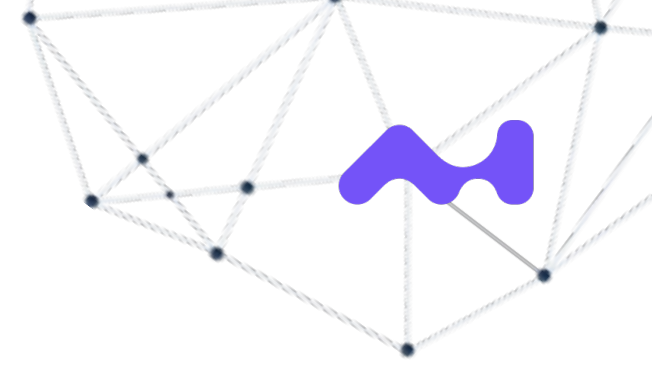
IBM T. J. Watson Research Center, Yorktown Heights, NY 10598 USA

Abstract

After a brief introduction to the principles and promise of quantum information processing, the requirements for the physical implementation of quantum computation are discussed. These five requirements, plus two relating to the communication of quantum information, are extensively explored and related to the many schemes in atomic physics, quantum optics, nuclear and electron magnetic resonance spectroscopy, superconducting electronics, and quantum-dot physics, for achieving quantum computing.



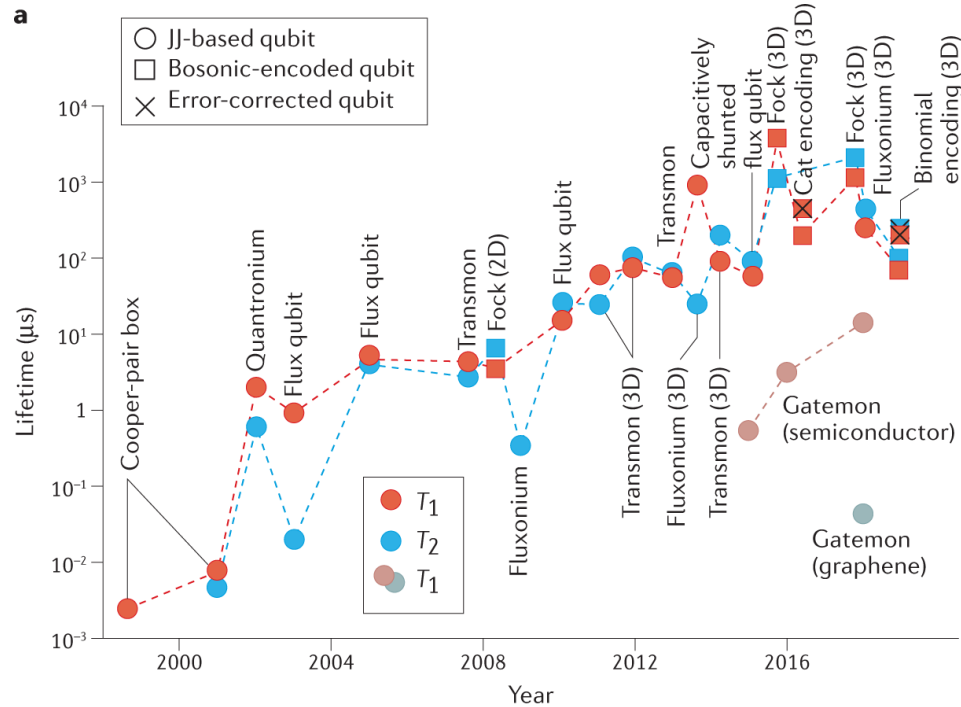
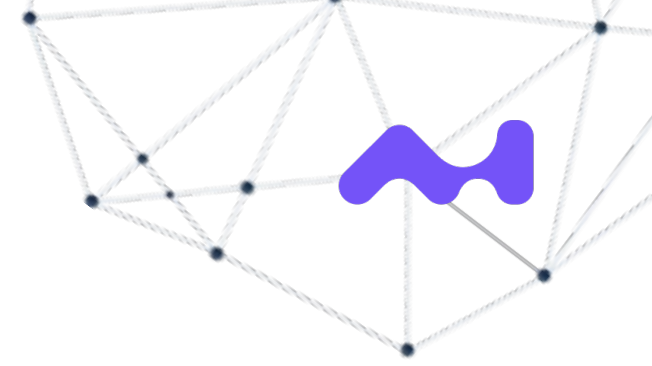
Qubits and How to Implement Them



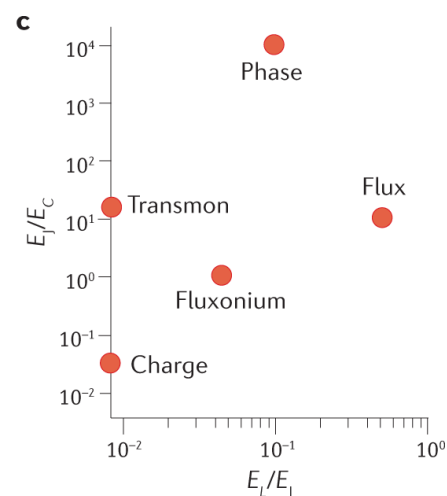
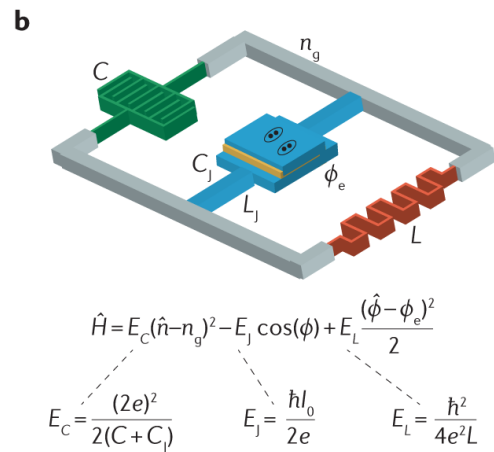
- “What is on the chip” differs
- Superconducting qubits (transmon, ...)
- Double quantum dots (in Si, Ge, ...)
- Photonic qubits
- Ions and neutral atoms
- Fullerenes, carbon nanotubes, etc.

Physical support	Name	Information support	$ 0\rangle$	$ 1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photons	Fock state	Vacuum	Single photon state
	Time-bin encoding	Time of arrival	Early	Late
Coherent state of light	Squeezed light	Quadrature	Amplitude-squeezed state	Phase-squeezed state
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron
Nucleus	Nuclear spin addressed through NMR	Spin	Up	Down
Optical lattices	Atomic spin	Spin	Up	Down
Josephson junction	Superconducting charge qubit	Charge	Uncharged superconducting island ($Q=0$)	Charged superconducting island ($Q=2e$, one extra Cooper pair)
	Superconducting flux qubit	Current	Clockwise current	Counterclockwise current
	Superconducting phase qubit	Energy	Ground state	First excited state
Singly charged quantum dot pair	Electron localization	Charge	Electron on left dot	Electron on right dot
Quantum dot	Dot spin	Spin	Down	Up
Gapped topological system	Non-abelian anyons	Braiding of Excitations	Depends on specific topological system	Depends on specific topological system
Vibrational qubit ^[10]	Vibrational states	Phonon/vibron	$ 01\rangle$ superposition	$ 10\rangle$ superposition
van der Waals heterostructure ^[11]	Electron localization	Charge	Electron on bottom sheet	Electron on top sheet

Qubits and How to Implement Them



- 1962: Josephson effect tunneling of superconducting Cooper pairs (Nobel Prize in Physics, 1973)
- Based on Josephson junction, superconducting qubits ess. implement a quantum oscillator
- Transmon qubits @ IBM
- Xmon @ Google
- Cca. At 10 mK



Qubits and How to Implement Them

- 1963: Quantum well with discrete energy values (Kroemer, Alferov, Kazarinov)
- Double quantum dots @ Intel, ...
- At 1K at Intel (?), up to 20 K (Myronov)

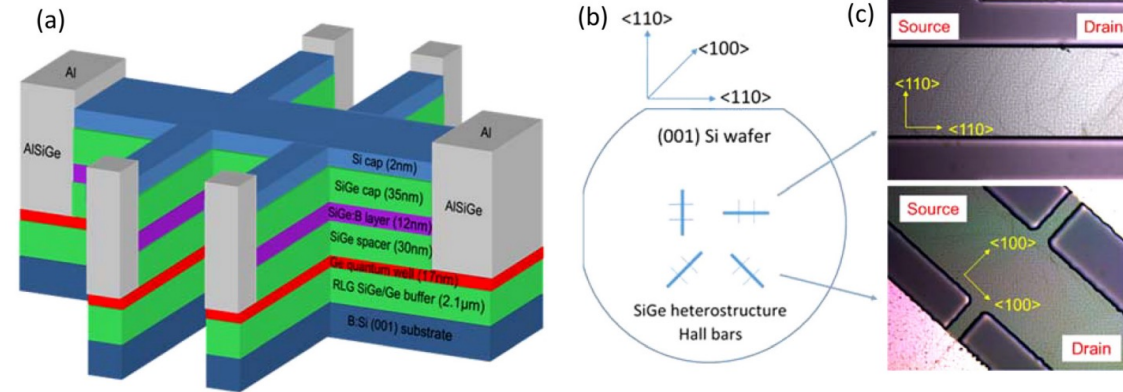
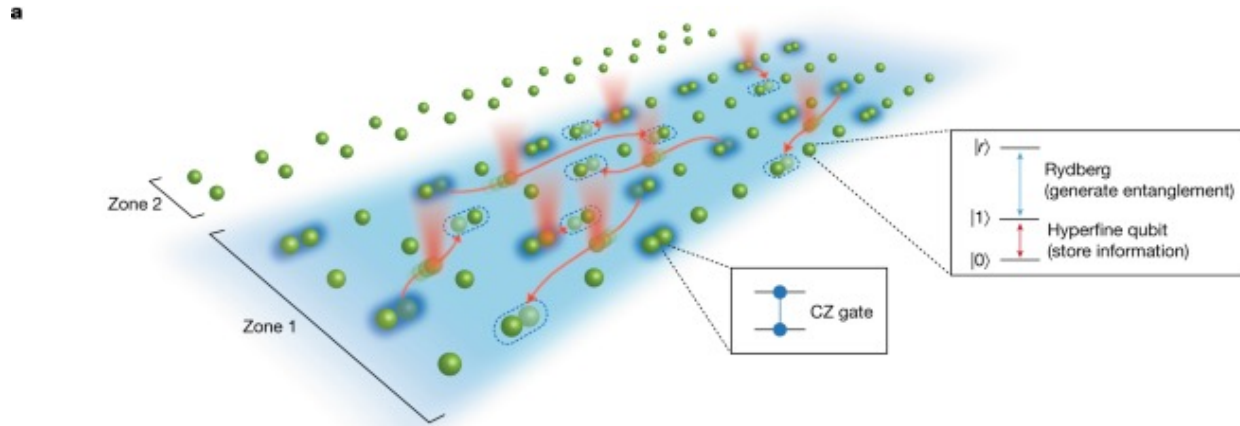
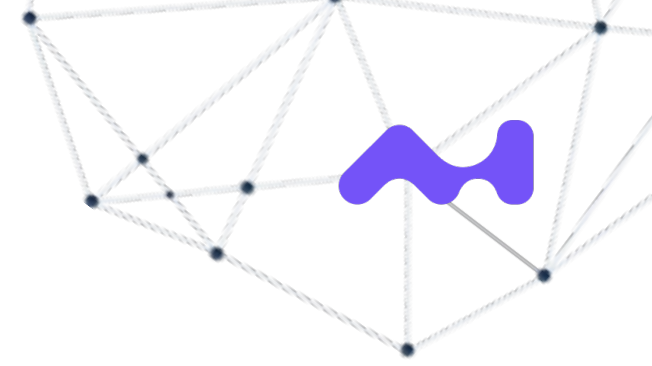


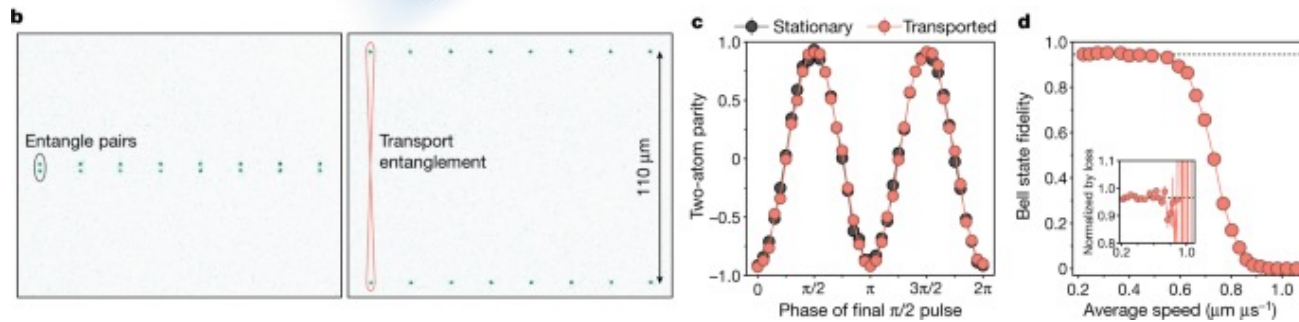
FIG. 1. (a) Schematic of the Hall bar device used, showing the composition of the heterostructure. (b) (001) plane of the wafer, illustrating the $\langle 110 \rangle$ and $\langle 100 \rangle$ directions. (c) Optical images of the Ge heterostructure Hall bars showing cross hatching from epitaxial growth. This pattern is aligned to the $\langle 110 \rangle$ directions.

Characteristics	Holes in strained Ge	Electrons in Si
Effective mass (m_0)	0.035	0.19 m
Coherence time (T_2^*)	150 μs	120 μs community accepts 20 μs
Rabi frequency	140 MHz	10 MHz
Single-qubit operation fidelity	99.3 %	99.9 %

Qubits and How to Implement Them



- Neutral atoms @ QuEra / Amazon / Harvard / ...
- 2D optical tweezer array
- Cca. at 25 μK (!)
- Entangled atoms cca. 110 μm apart
- Ions @ IoniQ / Alpine Quantum / Innsbruck / ...



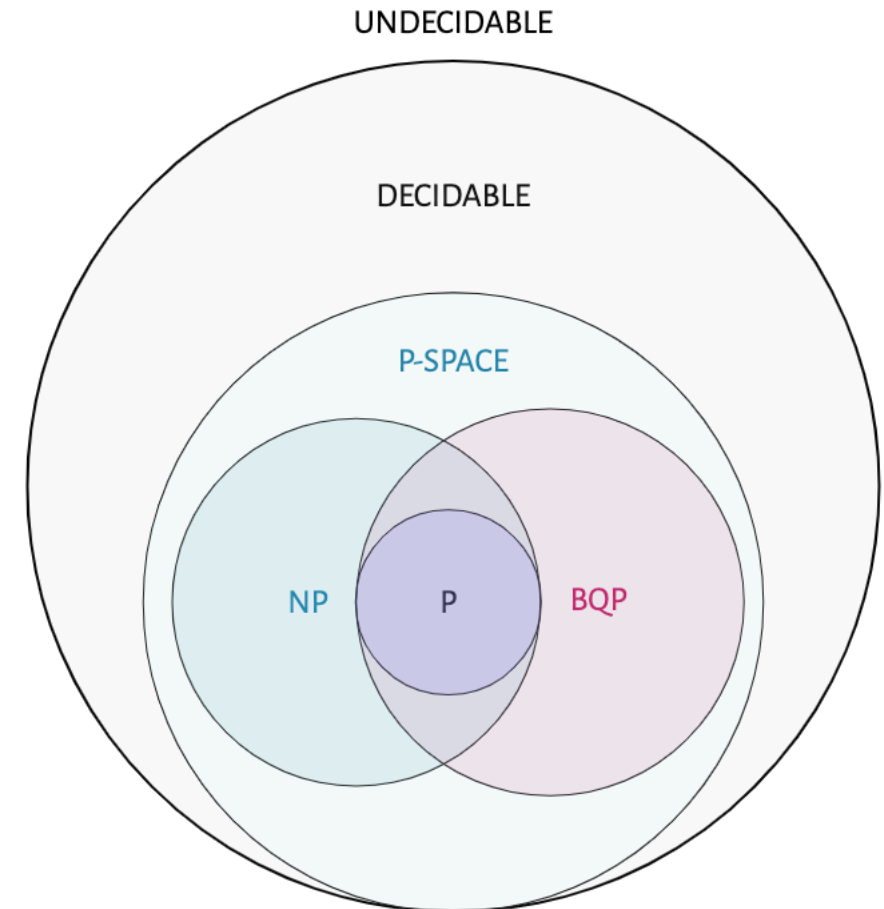
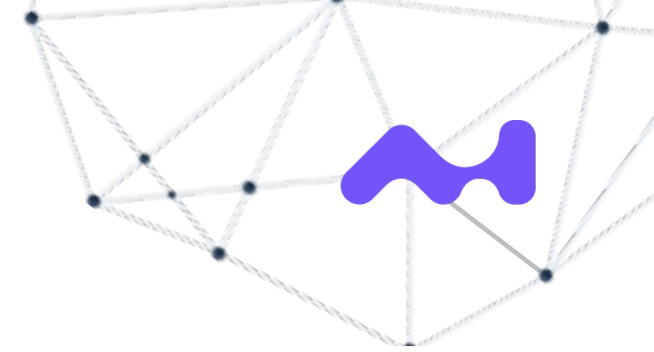
Quantum Computing

1. Motivation: "A social phenomenon"
2. Motivation: Opportunities and Limitations
3. Organization of the Course
4. Qubits and How to Implement them
5. A Theoretical Computer Science point of view
6. Three use cases in financial services



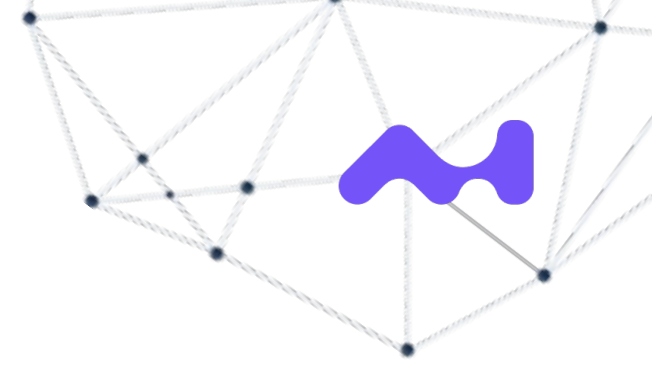
Computational Complexity

- P: a class of problems with certificates computable by a Turing machine in polynomial time. E.g. shortest path in a graph.
- NP: a class of problems with certificates verifiable by a Turing machine in polynomial time. E.g. the travelling salesman problem.
- BPP: a classical class of randomized algorithms.
- BQP: a "quantum equivalent" class to BPP.
- BQNP = QMA (Quantum Merlin Arthur): a "quantum equivalent" to NP. Specifically: A class of problems with polynomial-size quantum proof (a quantum state) that convinces a polynomial time quantum verifier (running on a quantum computer) with high probability.
- BQNP = QMA includes NP. It is not clear whether this is strict.



The zoo of classical and quantum complexity classes under the common assumptions that $NP \neq \text{P}$ and $NP \neq BQP$. Image credit: Jakub Marecek and Georgios Korpas.

Computational Complexity



Classical and Quantum Computation

A. Yu. Kitaev
A. H. Shen
M. N. Vyalıy

Graduate Studies
in Mathematics
Volume 47



American Mathematical Society

14.4. Local Hamiltonian is BQNP-complete.

Theorem 14.3. *The problem LOCAL HAMILTONIAN is BQNP-complete with respect to the Karp reduction.*

The rest of this section constitutes a proof of this theorem. The main idea goes back to Feynman [24]: replacing a unitary evolution by a time independent Hamiltonian (i.e., transition from the circuit to a local Hamiltonian).

Thus, suppose we have a circuit $U = U_L \cdots U_1$ of size L . We will assume that U acts on N qubits, the first m of which initially contain Merlin's message $|\xi\rangle$, the rest being initialized by 0. The gates U_j act on pairs of qubits.

14.4.1. The Hamiltonian associated with the circuit. It acts on the space

$$\mathcal{L} = \mathcal{B}^{\otimes N} \otimes \mathcal{C}^{L+1},$$

where the first factor is the space on which the circuit acts, whereas the second factor is the space of a step counter (clock). The Hamiltonian consists of three terms which will be defined later,

$$H = H_{\text{in}} + H_{\text{prop}} + H_{\text{out}}.$$

We are interested in the minimum eigenvalue of this Hamiltonian, or the minimum of the *cost function* $f(|\eta\rangle) = \langle \eta | H | \eta \rangle$ over all vectors $|\eta\rangle$ of unit length. We will try to arrange that the Hamiltonian has a small eigenvalue if and only if there exists a quantum state $|\xi\rangle \in \mathcal{B}^{\otimes m}$ causing U to output 1 with high probability. In such a case, the minimizing vector $|\eta\rangle$ will be related to that $|\xi\rangle$ in the following way:

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{j=0}^L U_j \cdots U_1 |\xi, 0\rangle \otimes |j\rangle.$$

In constructing the terms of the Hamiltonian, we will try to “enforce” this structure of the vector $|\eta\rangle$ by imposing “penalties” that increase the cost function whenever $|\eta\rangle$ deviates from the indicated form.

The term H_{in} corresponds to the condition that, at step 0, all the qubits but m are in state $|0\rangle$. Specifically,

$$(14.4) \quad H_{\text{in}} = \left(\sum_{s=m+1}^N \Pi_s^{(1)} \right) \otimes |0\rangle\langle 0|,$$

where $\Pi_s^{(\alpha)}$ is the projection onto the subspace of vectors for which the s -th qubit equals α . The second factor in this formula acts on the space of the counter. (Informally speaking, the term $\Pi_s^{(1)} \otimes |0\rangle\langle 0|$ “collects a penalty” by

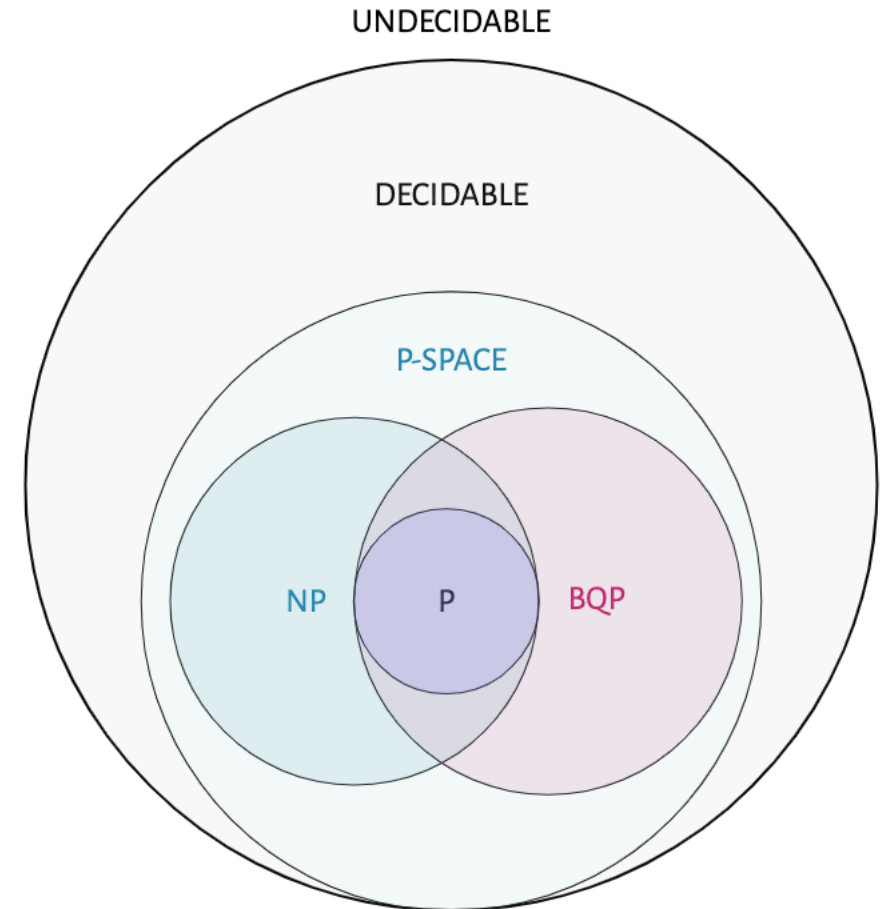
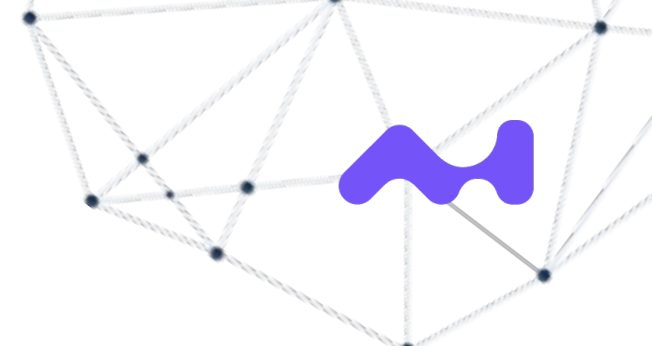
Computational Complexity

Let us consider a different class of problems, related to counting satisfying assignments, numerical integration, etc (#P):

- Classical Monte Carlo with N sample paths achieves error $O(1/\sqrt{N})$
- Quasi Monte Carlo methods on classical computers w/ error $O(\log(N)^s/N)$ for some s that may depend on dimension.
- Quantum replacements of Monte Carlo achieve error $O(1/N)$

This is often mis-understood in the hunt for elusive algorithms for NP-Complete problems!

Even $P^{\#P}$ is within PSPACE.



Quantum Computing

1. Motivation: "A social phenomenon"
2. Motivation: Opportunities and Limitations
3. Organization of the Course
4. Qubits and How to Implement them
5. A Theoretical Computer Science point of view
6. Three use cases in financial services



Three Use Cases

Cryptography

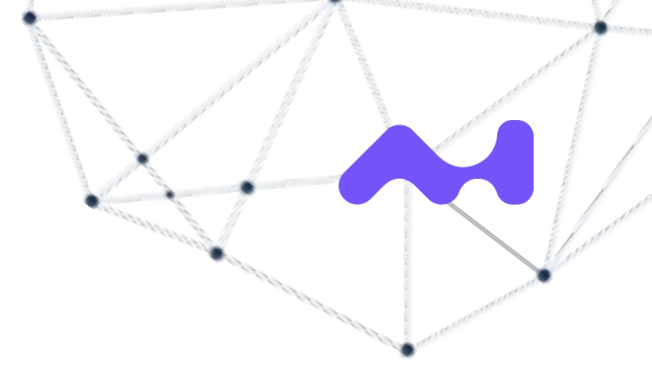
- The Big Scare
- Quantum Cryptography
- Post-quantum Cryptography

Simulation

- Monte Carlo Replacements

Optimization & Control

- Variational Algorithms?



arXiv > quant-ph > arXiv:2006.14510

Search...

Help | Advanced

Quantum Physics

[Submitted on 25 Jun 2020 (v1), last revised 28 Jan 2021 (this version, v3)]

Quantum Computing for Finance: State of the Art and Future Prospects

Daniel J. Egger, Claudio Gambella, Jakub Marecek, Scott McFaddin, Martin Mevissen, Rudy Raymond, Andrea Simonetto, Stefan Woerner, Elena Yndurain


This article outlines our point of view regarding the applicability, state-of-the-art, and potential of quantum computing for problems in finance. We provide an introduction to quantum computing as well as a survey on problem classes in finance that are computationally challenging classically and for which quantum computing algorithms are promising. In the main part, we describe in detail quantum algorithms for specific applications arising in financial services, such as those involving simulation, optimization, and machine learning problems. In addition, we include demonstrations of quantum algorithms on IBM Quantum back-ends and discuss the potential benefits of quantum algorithms for problems in financial services. We conclude with a summary of technical challenges and future prospects.

Comments: 24 pages

Subjects: **Quantum Physics (quant-ph)**; Statistical Finance (q-fin.ST)

Cite as: arXiv:2006.14510 [quant-ph]

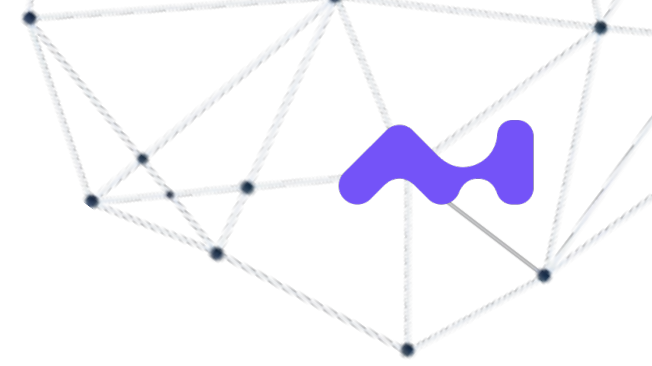
(or arXiv:2006.14510v3 [quant-ph] for this version)

<https://doi.org/10.48550/arXiv.2006.14510> 

Journal reference: IEEE Transactions on Quantum Engineering, vol. 1, pp. 1-24, 2020, Art no. 3101724

Related DOI: <https://doi.org/10.1109/TQE.2020.3030314> 

The Big Scare



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

Craig Gidney¹ and Martin Ekerå^{2,3}

¹Google Inc., Santa Barbara, California 93117, USA

²KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

³Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

Featured in Physics

Editors' Suggestion

Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits a Multimode Memory

Élie Gouzien and Nicolas Sangouard

Phys. Rev. Lett. **127**, 140503 – Published 28 September 2021

PhysICS See synopsis: [Far Fewer Qubits Required for “Quantum Memory” Quantum Computers](#)

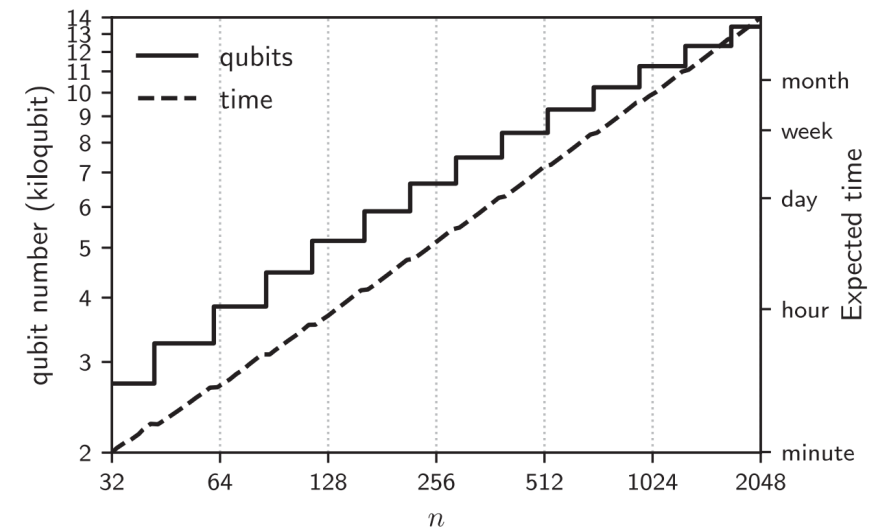


FIG. 2. Number of qubits in the processor and run-time to factor n -bit RSA integers with a computer architecture using a multimode memory.

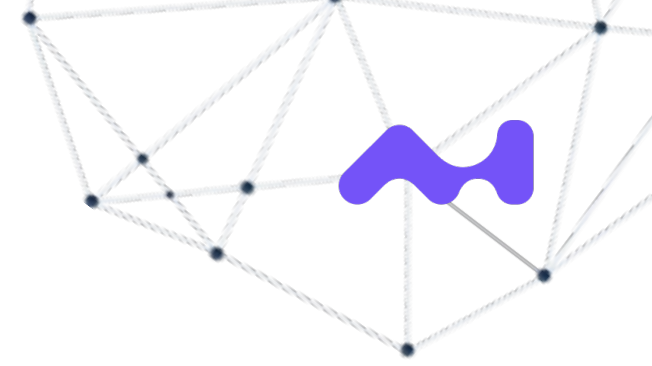
Quantum Cryptography

Long Distance QKD System

The Long Distance QKD System operates with a quantum channel in the telecom C-band for the longest possible range and highest possible secure key rate. It can tolerate limited bandwidths of multiplexed data within the C-band.

Key Features:

1. Typical key rate = 300 kb/s for 10dB loss
2. Range of up to 120km
3. Two fibers required
4. Efficient BB84 protocol with decoy states and phase encoding
5. Key failure probability of less than 10^{-10} equivalent to less than once in 30,000 years
6. Proprietary self-differencing semiconductor detectors

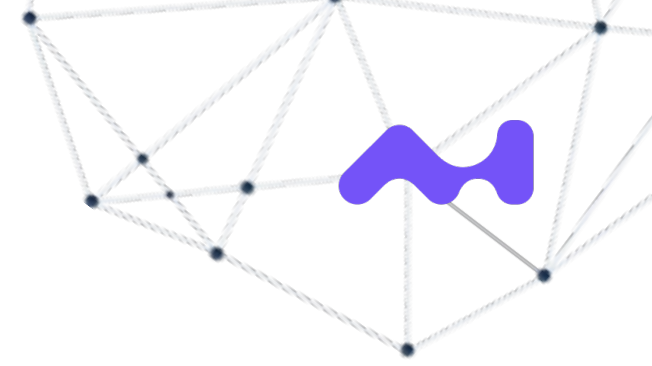


Why Toshiba QKD



We started research into quantum cryptography in 2003 at the Cambridge Research Laboratory of Toshiba Research Europe Limited. Since then we have demonstrated a number of notable world firsts. We were the first to announce quantum key distribution over 100 km of fiber in 2004 and the first with a continuous key rate exceeding 1 Mbit/second in 2010 and 10 Mbit/second in 2017.

Post-Quantum Cryptography



NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER



NIST IR 8413-upd1

PROJECTS

POST-QUANTUM CRYPTOGRAPHY

Post-Quantum Cryptography PQC



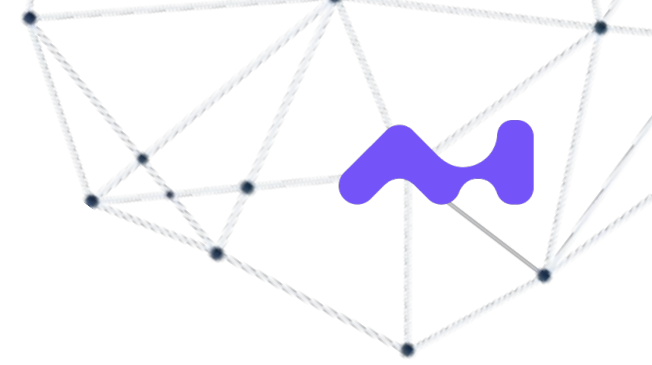
Selected Algorithms 2022

Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process

Selected Algorithms: Public-key Encryption and Key-establishment Algorithms

Algorithm	Algorithm Information	Submitters	Comments
CRYSTALS-KYBER	Zip File (7MB) IP Statements Website	Peter Schwabe Roberto Avanzi Joppe Bos Leo Ducas Eike Kiltz Tancrede Lepoint Vadim Lyubashevsky John M. Schanck	Submit Comment View Comments

Post-Quantum Cryptography



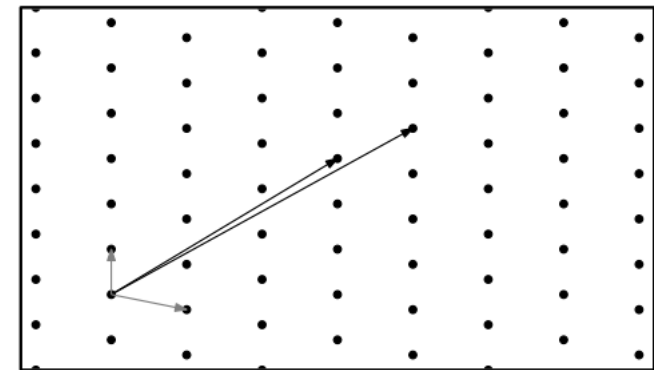
Kyber is based on lattice cryptography, which are NP-Hard and not known to be PSPACE-Hard. Non-trivially, the problem is related to SIVP: Given a lattice basis, find k linearly independent lattice vectors minimizing the maximum of their norms.

Worst-case to average-case reductions for module lattices

[Adeline Langlois](#) & [Damien Stehlé](#) 

[Designs, Codes and Cryptography](#) **75**, 565–599 (2015) | [Cite this article](#)

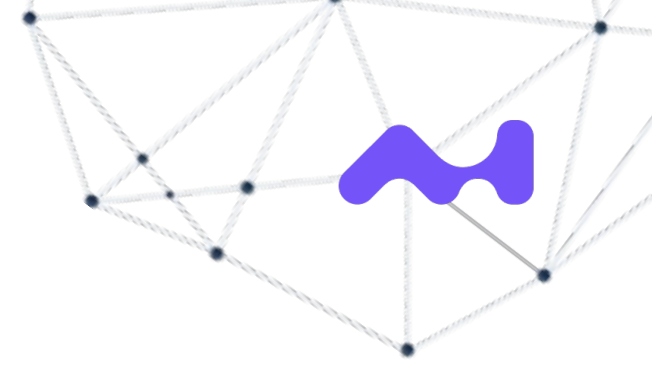
1912 Accesses | 171 Citations | 3 Altmetric | [Metrics](#)



Kyber is already being used:

- Cloudflare Interoperable, Reusable Cryptographic Library
- Amazon Web Services Key Management Service
- IBM's World's First Quantum Computing Safe Tape Drive (using Kyber and Dilithium).

Monte Carlo Replacements



Much of what banks do, boils down to Monte Carlo:

- Risk assessment and mandated by regulators
- Internal risk assessment
- Pricing of a variety of products (e.g. credit, European call options).

[Journals & Magazines](#) > [IEEE Transactions on Computers](#) > [Volume: 70 Issue: 12](#) ?

Credit Risk Analysis Using Quantum Computers

Publisher: IEEE

[Cite This](#)

[PDF](#)

What error do I get with N sample paths?

- Classical Monte Carlo methods $O(1/\sqrt{N})$
- Quasi-Monte-Carlo methods $O(\log(N)^5/N)$
- Quantum replacements $O(1/N^2)$

Option Pricing using Quantum Computers

Nikitas Stamatopoulos¹, Daniel J. Egger², Yue Sun¹, Christa Zoufal^{2,3}, Raban Iten^{2,3}, Ning Shen¹, and Stefan Woerner²

¹Quantitative Research, JPMorgan Chase & Co., New York, NY, 10017

²IBM Quantum, IBM Research – Zurich

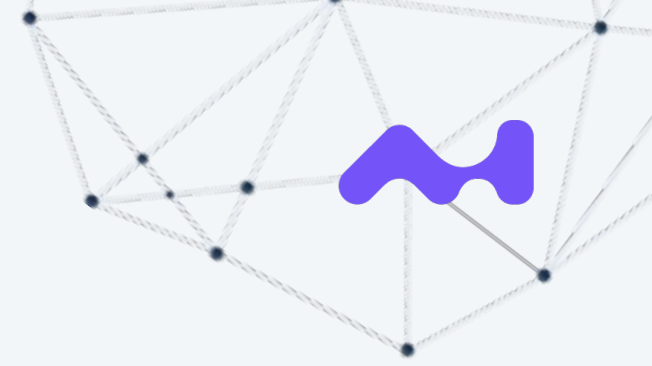
³ETH Zurich

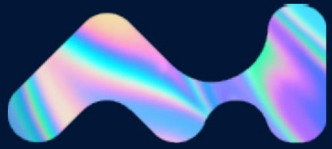
A Threshold for Quantum Advantage in Derivative Pricing

Shouvanik Chakrabarti^{1,2}, Rajiv Krishnakumar¹, Guglielmo Mazzola³, Nikitas Stamatopoulos¹, Stefan Woerner³, and William J. Zeng¹

Quantum Computing

1. Motivation: "A social phenomenon"
2. Motivation: Opportunities and Limitations
3. Organization of the Course
4. Qubits and How to Implement them
5. A Theoretical Computer Science point of view
6. Three use cases in financial services





AI CENTER
FEE CTU

www.aic.fel.cvut.cz

Artificial Intelligence Center
Faculty of Electrical Engineering
Czech Technical University in Prague

February 24th, 2023