

Quantum Computing Tech Talk



The State of Quantum Computing

Adam Bene Watts
Scientist-in-Residence
Quantum City, University of Calgary

July 23, 2025



**Quantum
City**



About Quantum City



Ecosystem Building:

Quantum City is building an ecosystem for quantum science and technology in Alberta, bringing together researchers, developers and adopters of quantum technology and services.



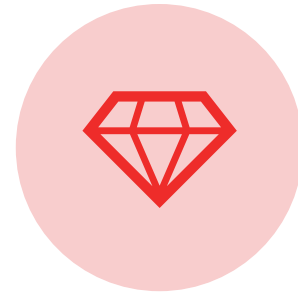
Partnership:

Established in 2022 with over \$100 million in investments, Quantum City is a partnership between the University of Calgary, Government of Alberta, and Mphasis.



Mission & Vision:

Our mission is to capture the benefits of quantum technology by creating adoption pathways. Quantum City's vision is to be the place where quantum technology becomes quantum solutions.



Values:

Transparency and authenticity, compassionate collaboration, ecosystem empowerment, and creative courage serve as the cornerstones in achieving our vision.

About me

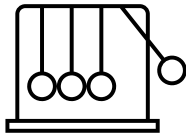
- **2011-2024:** Undergraduate in Math & Physics, PhD in Physics studying Quantum Computing, Postdoc studying Quantum Algorithms.
- **May 2024 – June 2025:** Scientist-in-Residence, Quantum Algorithms at Quantum City.
- **July 2025 – present:** Assistant Professor, Quantum Algorithms (Department of Math & Stats) at the University of Calgary.
- **Not a cybersecurity expert!**



About this talk

1. Introduction and motivation for quantum computing.
2. A timeline of the field.
3. Quantum Computing in the news.
4. Some intersection points between quantum technology and cybersecurity.

Recap: “Classical” Physics



Classical Mechanics ($\vec{F} = m\vec{a}$)

- Developed in the ~17th century.
- Describes collisions, orbits, mechanical motion.



Thermodynamics ($PV = nRT$)

- Developed in the ~19th century.
- Describes engines, heat, entropy.



Electricity and Magnetism ($V = IR$)

- Developed in the ~19th century.
- Describes electricity, magnetism, electric currents.

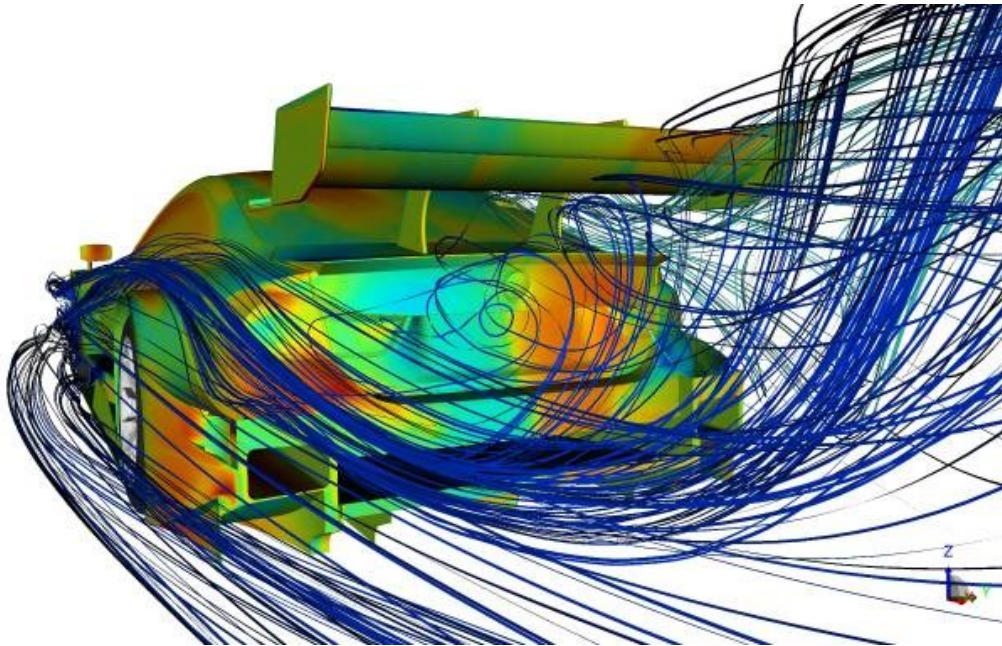
These theories describe most of the classical world around us.



In particular, they can describe computation!



... and computers are good at describing these theories.



The simulation argument.



The simulation argument.

“All computers can do about the same things”

Extended Church Turing Thesis: “Anything that can be efficiently computed by one computer can be efficiently computed by another.”

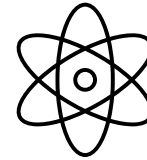
...but!

Modern Physics (early 1900s)



Relativity
($E = mc^2$)

- Describes things which are **moving very fast**, or which are **very heavy**.



Quantum Mechanics
($\hat{H}|\psi\rangle = E|\psi\rangle$)

- Describes things which are **very small**.

It seems that classical computers are **cannot efficiently simulate** quantum mechanics.

⇒ The **simulation argument breaks down** for a computer whose internals are quantum mechanical.

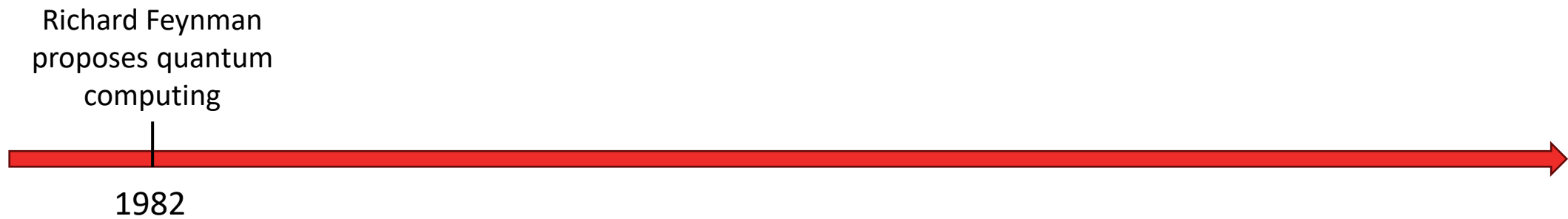
⇒ Such computers might be able to **efficiently solve problems** that regular computers can not!



“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.”

Richard Feynman
1981 (published in 1982)

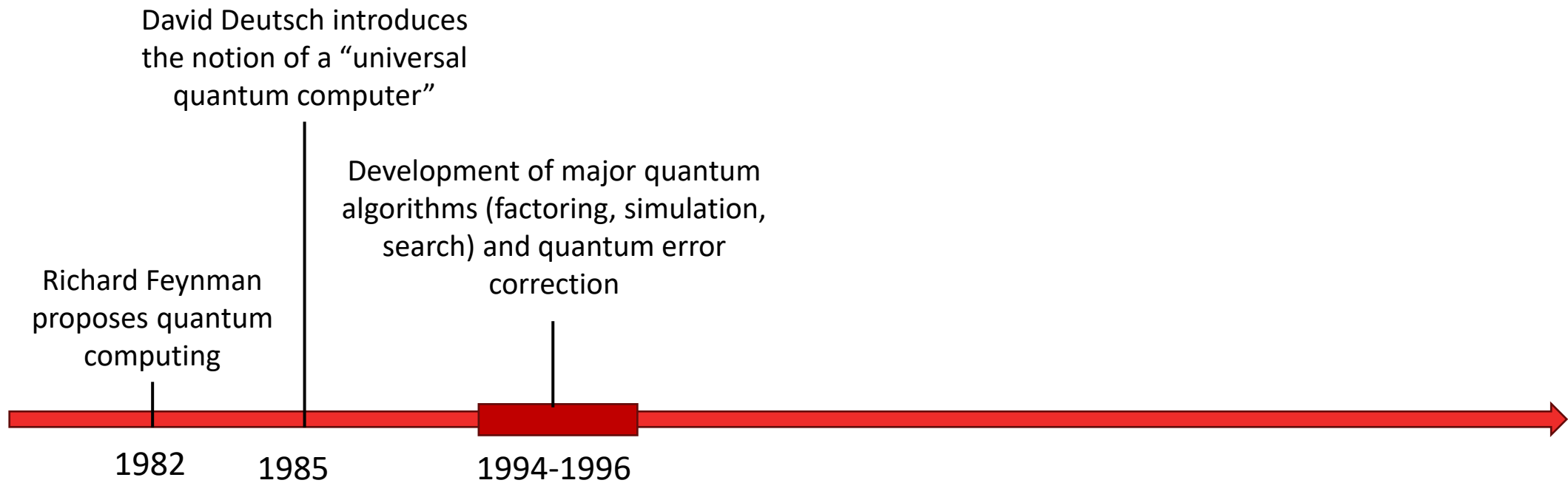
Quantum Computing Timeline



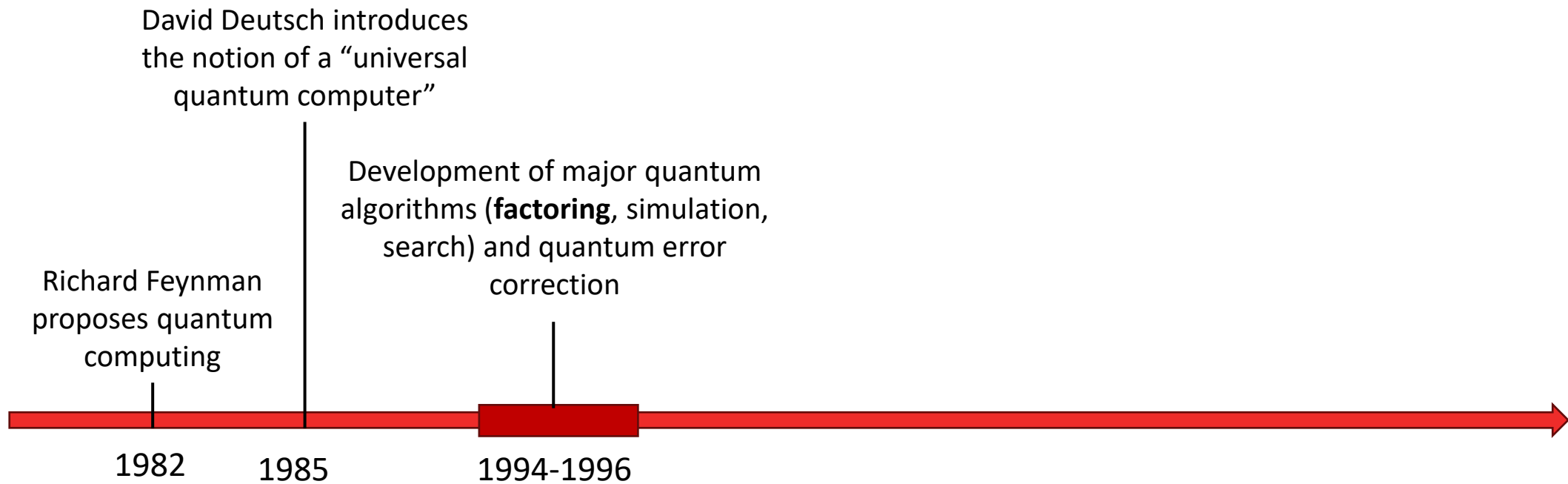
Quantum Computing Timeline



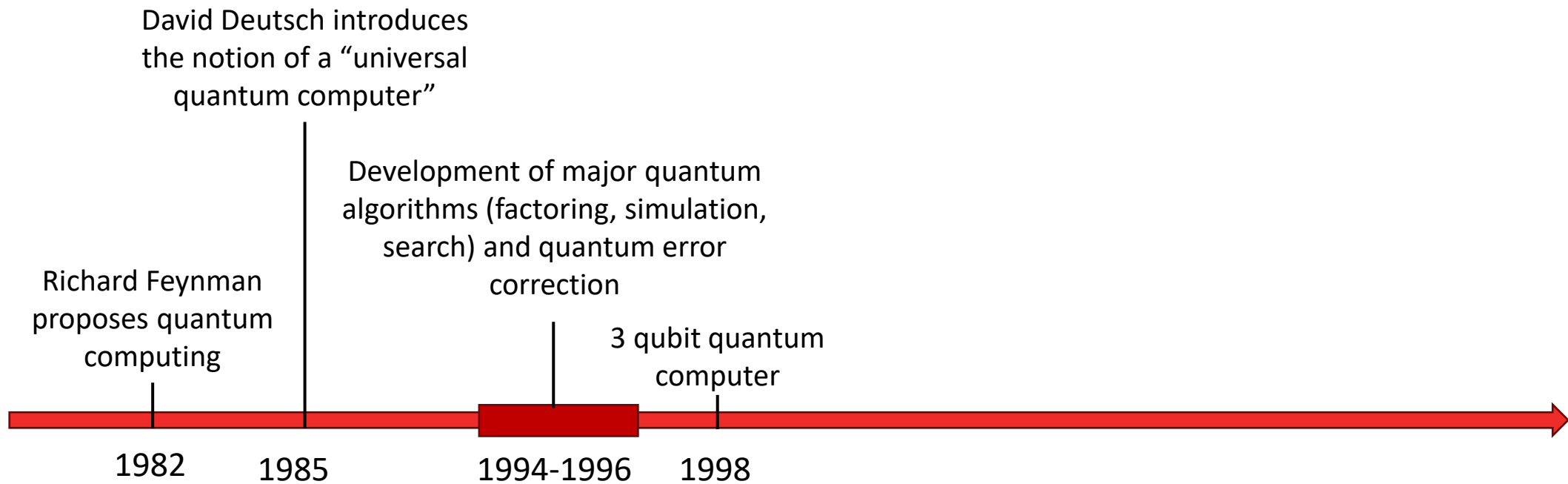
Quantum Computing Timeline



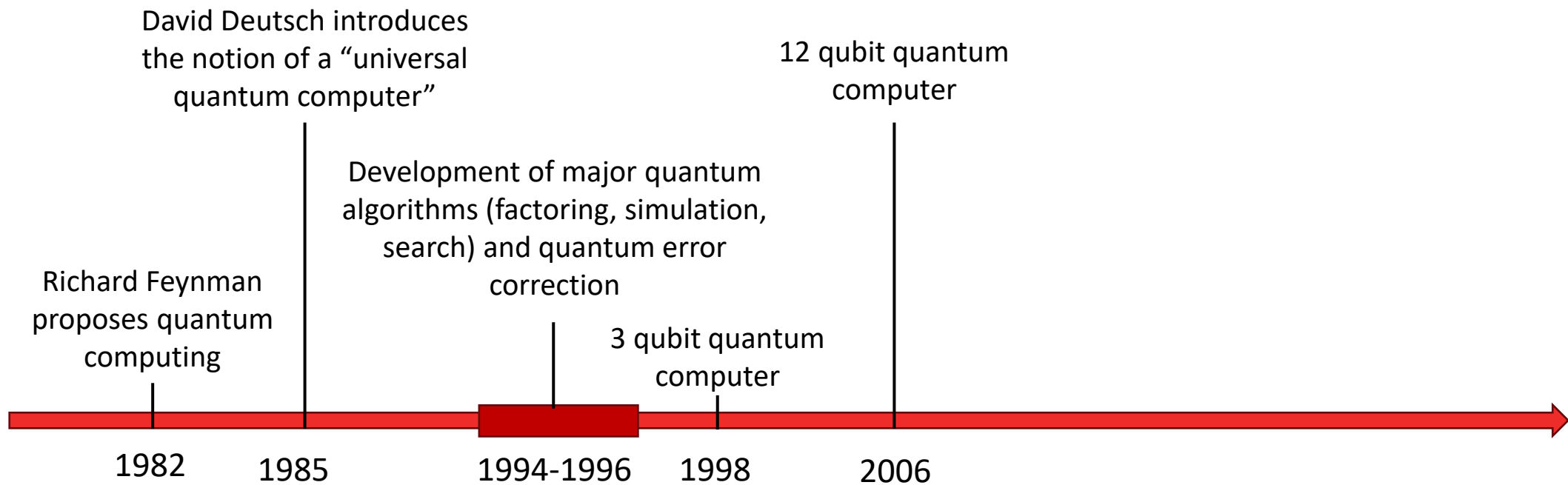
Quantum Computing Timeline



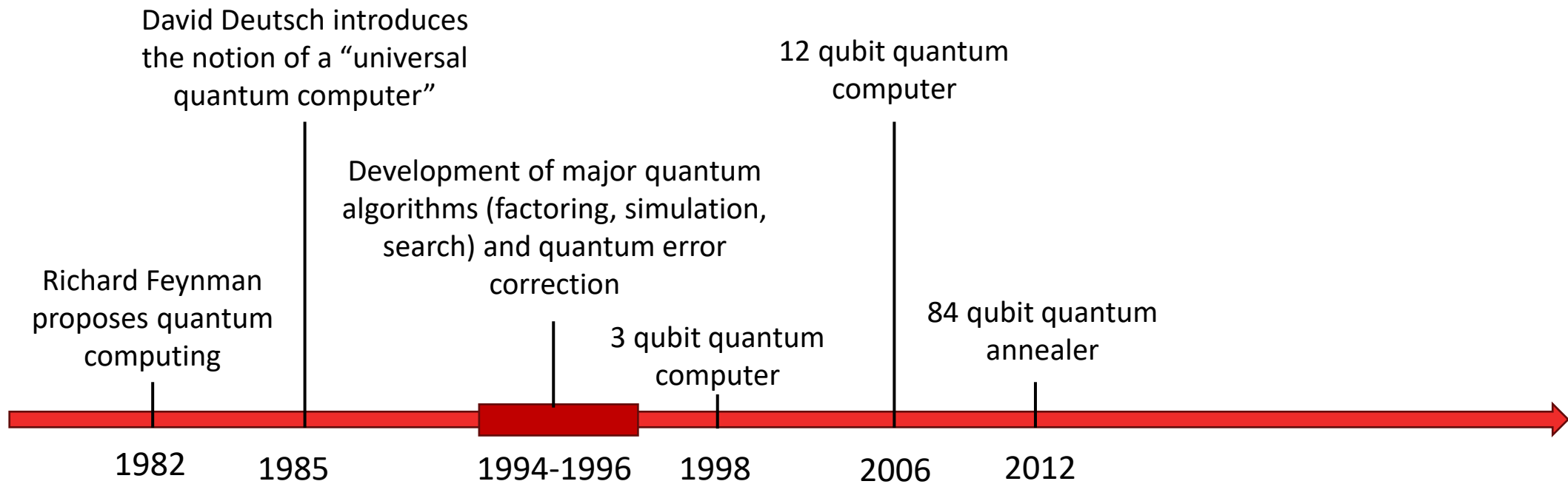
Quantum Computing Timeline



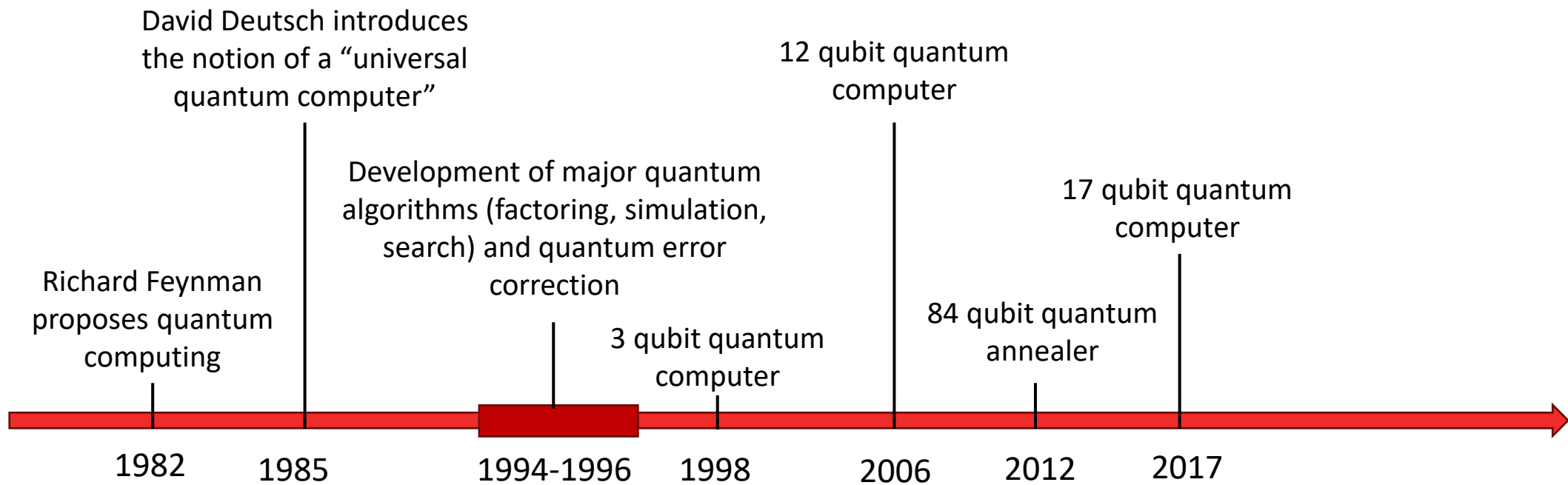
Quantum Computing Timeline



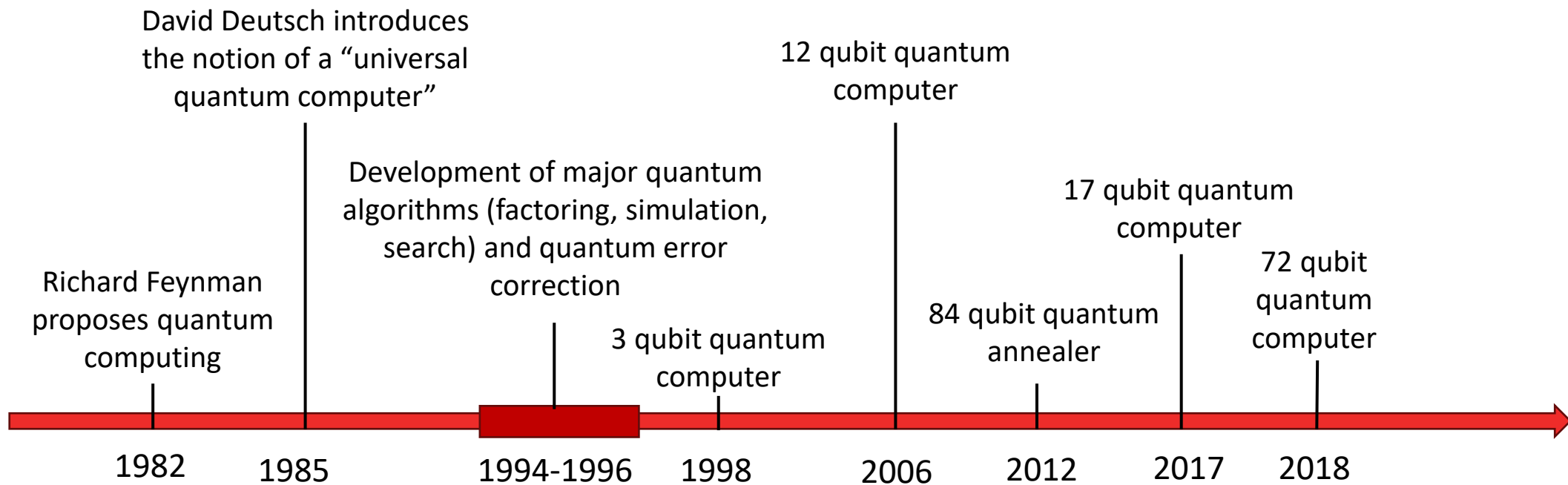
Quantum Computing Timeline



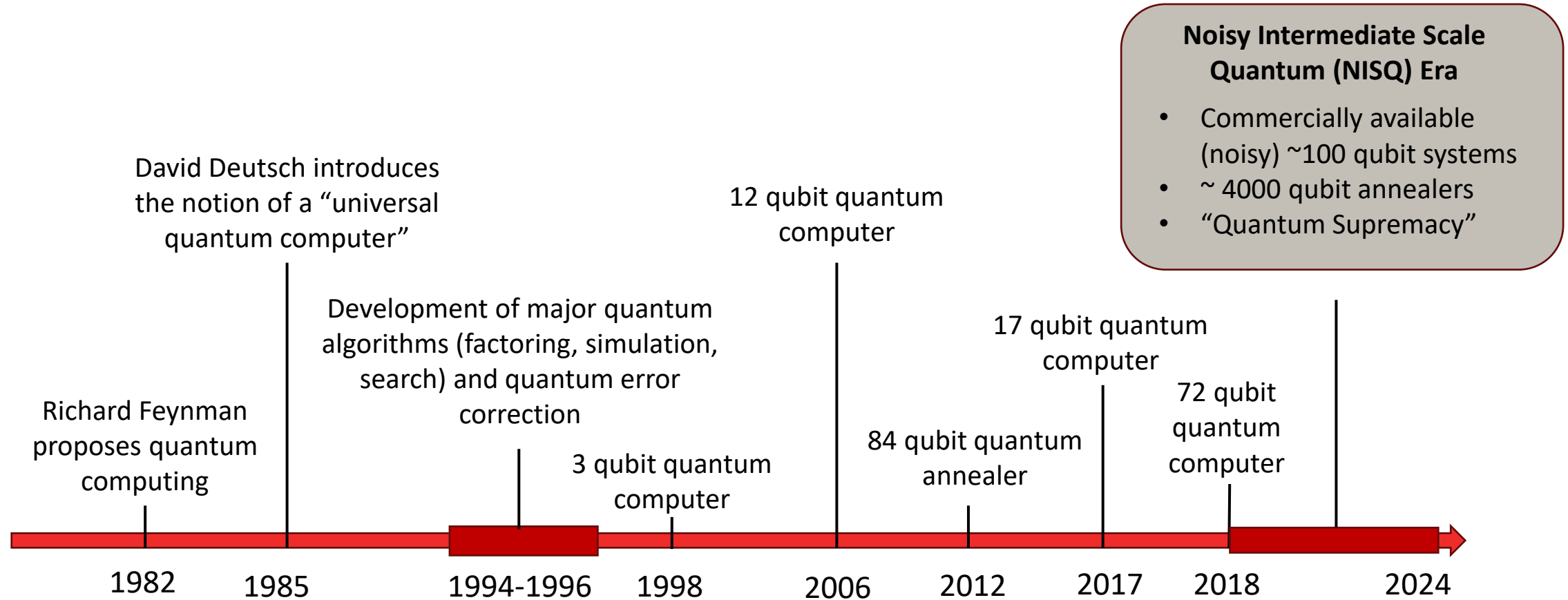
Quantum Computing Timeline



Quantum Computing Timeline



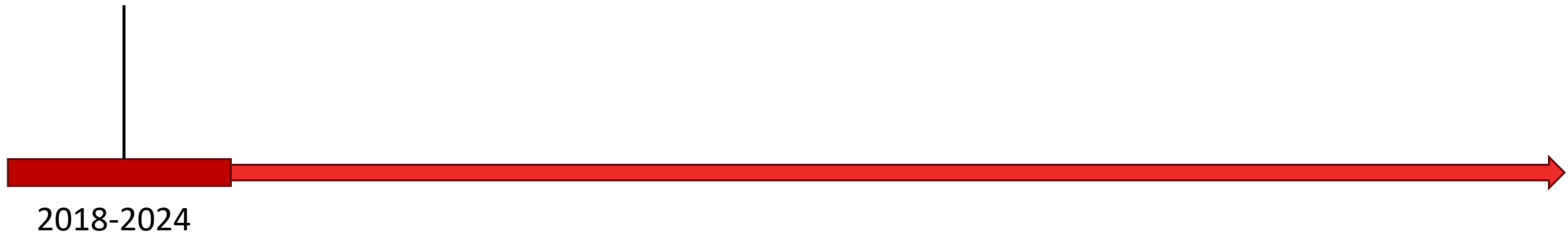
Quantum Computing Timeline



Quantum Computing Timeline (cont.)

Noisy Intermediate Scale Quantum (NISQ) Era

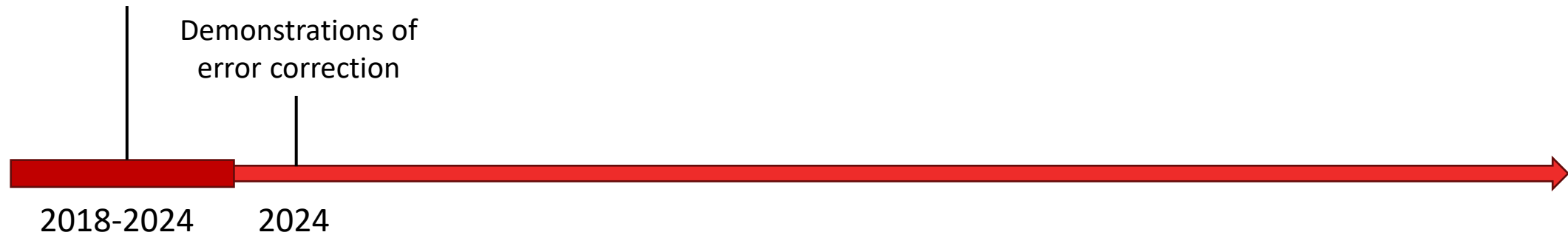
- Commercially available (noisy) ~100 qubit systems
- ~ 4000 qubit annealers
- “Quantum Supremacy”



Quantum Computing Timeline (cont.)

Noisy Intermediate Scale Quantum (NISQ) Era

- Commercially available (noisy) ~100 qubit systems
- ~ 4000 qubit annealers
- “Quantum Supremacy”



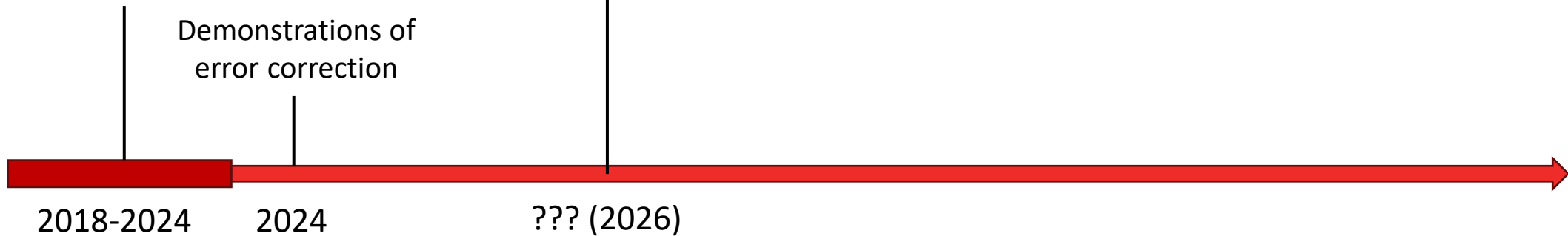
Quantum Computing Timeline (cont.)

Noisy Intermediate Scale Quantum (NISQ) Era

- Commercially available (noisy) ~100 qubit systems
- ~ 4000 qubit annealers
- “Quantum Supremacy”

Systems with ~1000's of noisy qubits.
“Quantum Utility”

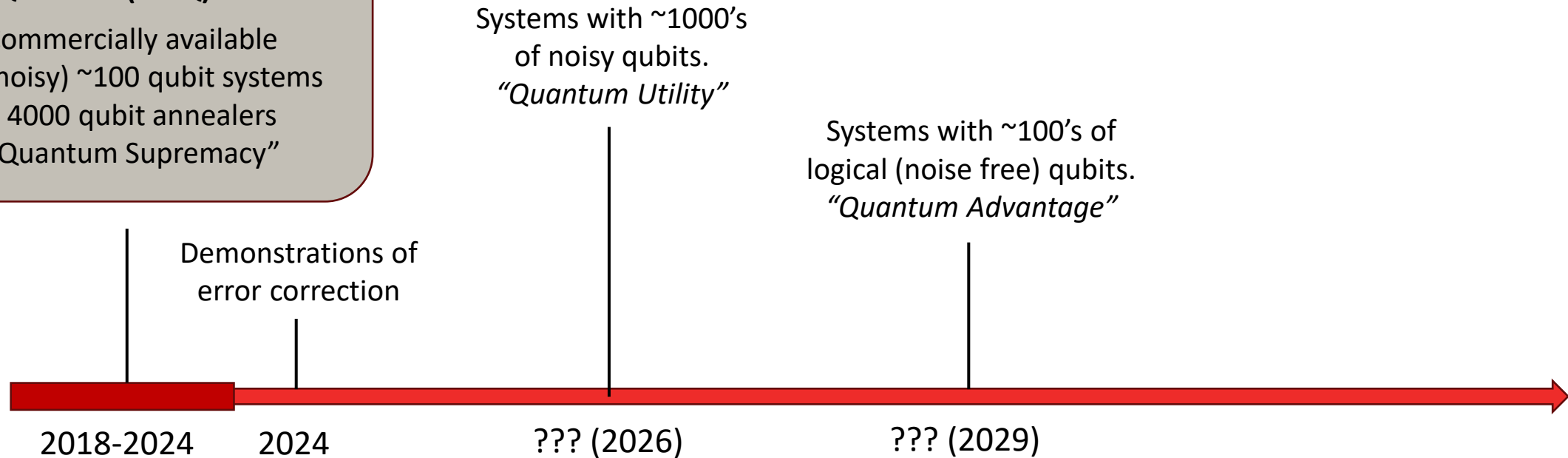
Demonstrations of error correction



Quantum Computing Timeline (cont.)

Noisy Intermediate Scale Quantum (NISQ) Era

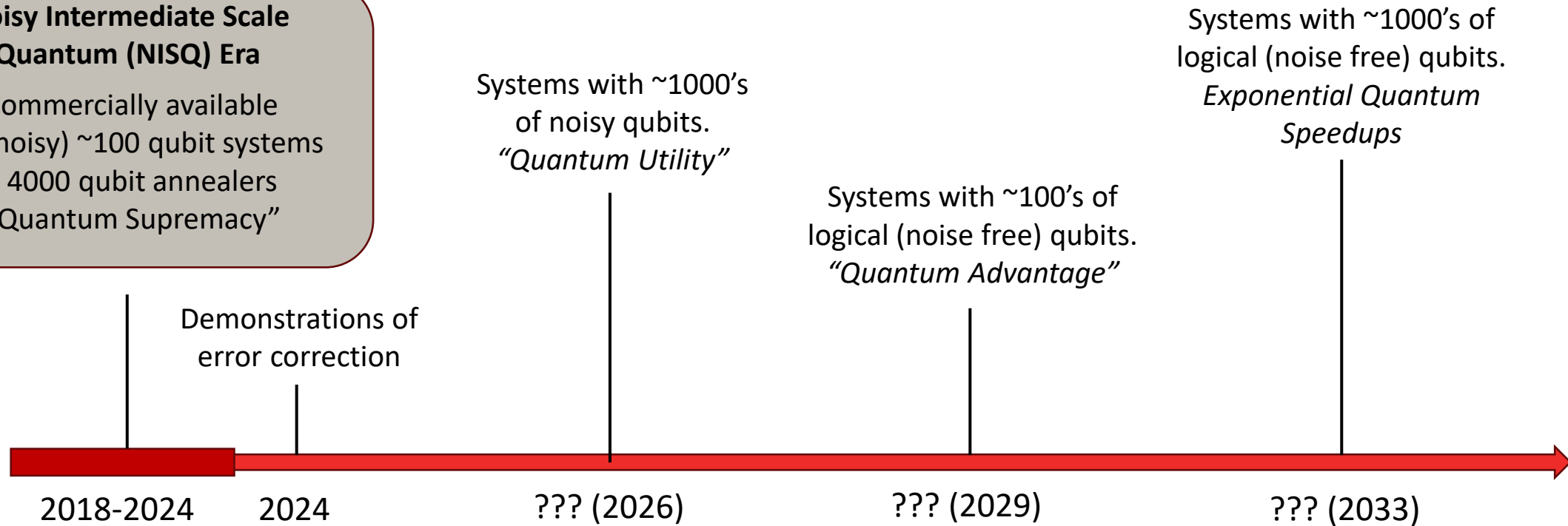
- Commercially available (noisy) ~100 qubit systems
- ~ 4000 qubit annealers
- “Quantum Supremacy”



Quantum Computing Timeline (cont.)

Noisy Intermediate Scale Quantum (NISQ) Era

- Commercially available (noisy) ~100 qubit systems
- ~ 4000 qubit annealers
- “Quantum Supremacy”



Quantum Computing in the news

Quantum Supremacy

Quantum Supremacy

GOOGLE PUBLISHES LANDMARK QUANTUM SUPREMACY CLAIM

The company says that its quantum computer is the first to perform a calculation that would be **practically impossible for a classical machine.**

By Elizabeth Gibney

Scientists at Google say that they have achieved quantum supremacy, a long-awaited milestone in quantum computing. The announcement, published in *Nature* on 23 October, follows a leak of an early version of the paper five weeks ago, which Google did not comment on at the time.

In a world first, a team led by John Martinis, an experimental physicist at the University of California, Santa Barbara, and Google in Mountain View, California, says that its quantum computer carried out a specific calculation that is beyond the practical capabilities of regular,

'classical' machines (F. Arute *et al.* *Nature* **574**, 505–510; 2019). **The same calculation would take even the best classical supercomputer 10,000 years to complete,** Google estimates.

Quantum supremacy has long been seen as a milestone because it proves that quantum computers can outperform classical computers, says Martinis. Although the advantage has now been proved only for a very specific case, it shows physicists that quantum mechanics works as expected when harnessed in a complex problem.

"It looks like Google has given us the first experimental evidence that quantum speed-up is achievable in a real-world system," says

Michelle Simmons, a quantum physicist at the University of New South Wales in Sydney, Australia.

The feat was first reported in September by the *Financial Times* and other outlets, after an early version of the paper was leaked on the website of NASA, which collaborates with Google on quantum computing, before being quickly taken down. At that time, the company did not confirm that it had written the paper, nor would it comment on the stories.

Although the calculation Google chose – checking the outputs from a quantum random-number generator – has limited practical applications, "the scientific achievement is

Nature | Vol 574 | 24 October 2019 | **461**

Quantum Supremacy

GOOGLE PUBLISHES LANDMARK PAPER: THE NEW LIGHT-BASED QUANTUM COMPUTER JIUZHANG HAS ACHIEVED QUANTUM SUPREMACY

The company says the calculation that would

A second type of quantum device performed a calculation impossible for a traditional computer

By Elizabeth Gibney

By [Emily Conover](#)

Scientists at Google say they have achieved quantum supremacy, an awaited milestone in quantum computing. The announcement came in *Nature* on 23 October, of an early version of the paper for which Google did not comment.

In a world first, a team led by John Martinis, an experimental physicist at the University of California, Santa Barbara, and Google's Quantum AI team in Mountain View, California, says that the quantum computer carried out a specific calculation that is beyond the practical capabilities of any classical computer.

DECEMBER 3, 2020 AT 2:00 PM - MORE THAN 2 YEARS AGO

A new type of quantum computer has proven that it can reign supreme, too.

A photonic quantum computer, which harnesses particles of light, or photons, **performed a calculation that's impossible for a conventional computer**, researchers in China report online December 3 in *Science*.

That milestone, known as quantum supremacy, has been met only once before, in 2019 by [Google's quantum computer](#) (*SN*: 10/23/19). Google's computer, however, is based on superconducting materials, not photons.

...crist at
...dney,

...iber by
...i, after
...ed on
...s with
...being
...mpany
...paper,

...rose —
...m ran-
...actical
...ent is

| 461

Quantum Supremacy

GOOGLE PUBLISHES LANDMARK SUPREMACY

The company says the calculation that would

By Elizabeth Gibney

Scientists at Google say they have achieved quantum supremacy, an awaited milestone in quantum computing. The announcement came in *Nature* on 23 October, of an early version of the paper for which Google did not comment.

In a world first, a team led by John Martinis, an experimental physicist at the University of California, Santa Barbara, and Google's Quantum AI team in Mountain View, California, says that their quantum computer carried out a specific calculation that is beyond the practical capabilities of

The new light-based

quantum computer. Jiuzhang has achieved quantum supremacy.

A second type of quantum device performed the calculation faster than a traditional computer.

By Emily Conover

DECEMBER 3, 2020 AT 2:00 PM - MORE THAN 100 COMMENTS

A new type of quantum computer has achieved quantum supremacy, too.

A photonic quantum computer using photons, [performed a calculation](#) that researchers in China say is beyond the practical capabilities of classical computers.

That milestone, known as quantum supremacy, was achieved for the first time once before, in 2019 by Google's quantum computer, however, is not photons.

Quantum computational advantage with a programmable photonic processor


<https://doi.org/10.1038/s41586-022-04725-x>

Received: 12 November 2021

Accepted: 5 April 2022

Published online: 1 June 2022

Open access

 Check for updates

Lars S. Madsen^{1,3}, Fabian Laudenbach^{1,3}, Mohsen Falamarzi^{1,3}, Askarani^{1,3}, Fabien Rortais¹, Trevor Vincent¹, Jacob F. F. Bulmer¹, Filippo M. Miatto¹, Leonhard Neuhaus¹, Lukas G. Helt¹, Matthew J. Collins¹, Adriana E. Lita², Thomas Gerrits², Sae Woo Nam², Varun D. Vaidya¹, Matteo Menotti¹, Ish Dhand¹, Zachary Vernon¹, Nicolás Quesada^{1,3} & Jonathan Lavoie^{1,3}

A quantum computer attains computational advantage when outperforming the best classical computers running the best-known algorithms on well-defined tasks. No photonic machine offering programmability over all its quantum gates has demonstrated quantum computational advantage: previous machines^{1,2} were largely restricted to static gate sequences. Earlier photonic demonstrations were also vulnerable to spoofing³, in which classical heuristics produce samples, without direct simulation, lying closer to the ideal distribution than do samples from the quantum hardware. Here we report quantum computational advantage using Borealis, a photonic processor offering dynamic programmability on all gates implemented. We carry out Gaussian boson sampling⁴ (GBS) on 216 squeezed modes entangled with three-dimensional connectivity⁵, using a time-multiplexed and photon-number-resolving architecture. On average, it would take more than 9,000 years for the best available algorithms and supercomputers to produce, using exact methods, a single sample from the programmed distribution, whereas Borealis requires only 36 μ s. This runtime advantage is over 50 million times as extreme as that reported from earlier photonic machines. Ours constitutes a very large GBS experiment, registering events with up to 219 photons and a mean photon number of 125. This work is a critical milestone on the path to a practical quantum computer, validating key technological features of photonics as a platform for this goal.

Quantum Supremacy

GOOGLE PUBLISHES LANDMARK SUPREMACY

The company says the calculation that would

By Elizabeth Gibney

Scientists at Google say they have achieved quantum supremacy, an awaited milestone in quantum computing. The announcement came in *Nature* on 23 October, of an early version of the paper for which Google did not comment.

In a world first, a team led by John Martinis, an experimental physicist at the University of California, Santa Barbara, and Google's John Martinis, says that the computer carried out a specific calculation that is beyond the practical capabilities of

The new light-based quantum computer, Jiuzhang has achieved quantum supremacy.

A second type of quantum device performed the calculation faster than a traditional computer

By Emily Conover

DECEMBER 3, 2020 AT 2:00 PM - MORE THAN 100 COMMENTS

A new type of quantum computer has achieved quantum supremacy, too.

A photonic quantum computer using photons, performed a calculation that a classical computer cannot. That milestone, known as quantum supremacy, was first achieved once before, in 2019 by Google's computer, however, is not photons.


<https://doi.org/10.1038/s41586-022-04725-x>

Received: 12 November 2021

Accepted: 5 April 2022

Published online: 1 June 2022

Open access

 Check for updates

China achieves quantum supremacy claim with new chip 1 quadrillion times faster than the most powerful supercomputers

News

By Alan Bradley published March 13, 2025

This new superconducting prototype quantum processor achieved benchmarking results to rival Google's new Willow QPU.

Researchers in China have developed a quantum processing unit (QPU) that is 1 quadrillion (10^{15}) times faster than the best supercomputers on the planet.

The new prototype 105-qubit chip, dubbed "Zuchongzhi 3.0," which uses superconducting qubits, represents a significant step forward for quantum computing, scientists at the University of Science and Technology of China (USTC) in Hefei said.

It rivals the benchmarking results set by Google's latest Willow QPU in December 2024 that allowed scientists to stake a claim for quantum supremacy — where quantum computers are more capable than the fastest supercomputers — in lab-based benchmarking.

The new chip constitutes a very large QBS experiment, registering events with up to 219 photons and a mean photon number of 125. This work is a critical milestone on the path to a practical quantum computer, validating key technological features of photonics as a platform for this goal.

Quantum Advantage

Quantum Advantage

Quantum Case Files – Real-World Impact: Quantum Computing In Production – Streamlining Logistics For Pattison Food Group

October 26, 2024

Welcome to the *Quantum Case Files: Real-World Impact* series. At the Quantum Innovation Summit, our mission is not only to foster quantum technology adoption but to share real, in-production examples that highlight its transformative potential. This series is dedicated to illuminating case studies that demonstrate how quantum technology is **Pattison Food Group** COVID-19 pandemic.

Quantum Computing Transforms Logistics for Pattison Food Group (PFG)

During the initial wave of the pandemic, online orders surged, stressing logistics networks and increasing demand for timely delivery of essential goods. For **Pattison Food Group (PFG)**, Canada's largest retailer of food and healthcare products with over 100 retail locations across western Canada, coordinating deliveries at this volume was challenging. Manual scheduling, previously handled by a team, was no longer sustainable as it required up to 80 hours of work each week—an approach that could not keep pace with the growing demand.

The Challenge: Meeting Pandemic-Era Demand with Optimized Logistics

Quantum Advantage

Quantum Case Files – Real-World Impact: Quantum Computing In Production – Streamlining

October 26, 2024

Welcome to the *Quantum Case Files*: Summit, our mission is not only to focus on production examples that highlight its illuminating case studies that demonstrate COVID-19 pandemic.

Quantum Computing Transforms I

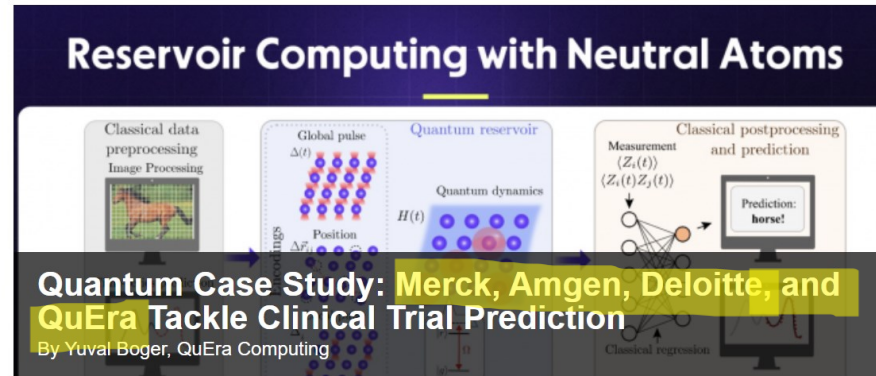
During the initial wave of the pandemic, increasing demand for timely delivery in Canada's largest retailer of food and beverages in western Canada, coordinating deliveries previously handled by a team, was now done each week—an approach that could not

The Challenge: Meeting Pandemic-Era



Since 1987 - Covering the Fastest Computers in the World and the People Who Run Them

- ▼ Topics
- ▼ Sectors
- ▼ QCwire Home
- ▼ QCwire Subscribe
- ▼ Exascale
- ▼ Specials
- ▼ Resource Library
- ▼ Podcast
- ▼ Events
- ▼ Job Bank
- ▼ About



April 10, 2025

Editor's Note: Have you heard of Quantum Reservoir Computing (QRC)? It's an interesting twist on classical [reservoir computing](#). Both are machine learning frameworks and I've appended more information at the end of the article, including an explanatory graphic drawn from a QuEra [paper](#) on the topic (Large-scale quantum reservoir learning with an analog quantum computer) and a link to another [paper](#) (Robust Quantum Reservoir Computing for Molecular Property Prediction.)

The POC project with Merck KGaA, Amgen, Deloitte, and QuEra presented below compared the ability of QRC with current classical methods to predict molecular properties from relatively small datasets, a common challenge in drug discovery. QRC's success in this project suggests it might be a valuable tool in many similar data-constrained areas.

Quantum Advantage

Quantum Case Files – Real-World Impact: Quantum Computing I Production – Streamlining

October 26, 2024

Welcome to the *Quantum Case Files*: Summit, our mission is not only to focus on production examples that highlight its illuminating case studies that demonstrate COVID-19 pandemic.

Quantum Computing Transforms I

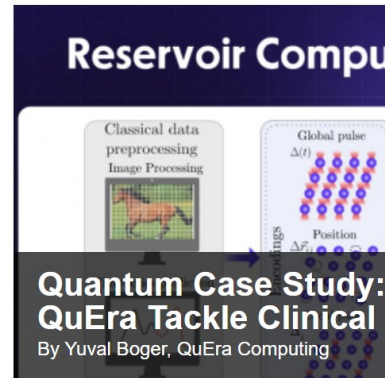
During the initial wave of the pandemic, increasing demand for timely delivery in Canada's largest retailer of food and home goods in western Canada, coordinating deliveries previously handled by a team, was now done each week—an approach that could not

The Challenge: Meeting Pandemic-Era



Since 1987 - Covering the Fastest Computers in the World and the People Who Run Them

- ✓ Topics
- ✓ Sectors
- ✓ QCwire Home
- ✓ QCwire Subscribe
- ✓ Exascale
- ✓ Specials
- ✓ Resource Library
- ✓ Podcast
- ✓ Events
- ✓ Job Bank
- ✓ About



April 10, 2025

Editor's Note: Have you heard of (or seen) an interesting twist on classical reinforcement learning frameworks and I've appeared in an article, including an explanatory graphic on the topic (Large-scale quantum reservoir computing) and a link to another piece for Molecular Property Prediction.

The POC project with Merck KGaA, below compared the ability of QRC to predict molecular properties from relatively small datasets. QRC's success in this area is a tool in many similar data-constrained areas.

The dawn of quantum advantage

The first claims of quantum advantage are emerging, but how will we know when it's really arrived? Researchers from IBM® and quantum startup Pasqal explore this and other questions in a new white paper now on arXiv.

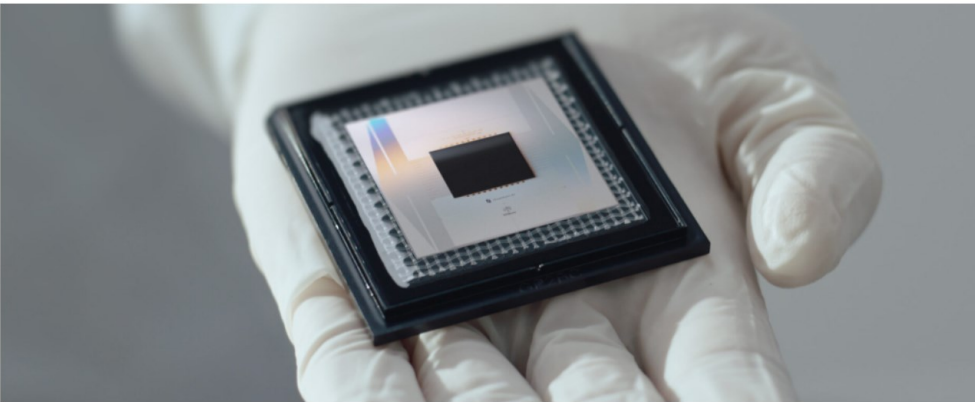
Quantum computing is about to enter an important stage — the era of quantum advantage. The first claims of quantum advantage are emerging, and over the next few years, we expect researchers and developers to continue presenting compelling hypotheses for quantum advantages. In turn, the broader community will either disprove these hypotheses with cutting-edge techniques — or the advantage holds.

Put simply, quantum advantage means that a quantum computer can run a computation more accurately, cheaply, or efficiently than a classical computer. Between now and the end of 2026, we predict that the quantum community will have uncovered the first quantum advantages. But there's more to it than that.

Fault Tolerant Quantum Computing

Google's New Chip Could Crack One of Quantum Computing's Biggest Problems

TECH 11 December 2024 By DAVID NIELD



Google's new quantum chip Willow. (Google)

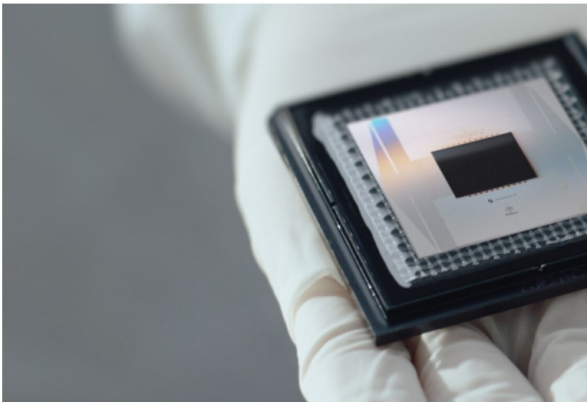
In spite of [the advances made](#) towards making [quantum computers](#) practical, qubit-based systems remain unstable and highly vulnerable to errors, something Google may have taken a major step towards fixing.

Through a newly unveiled quantum chip called Willow, Google engineers have passed a significant milestone in error handling. Specifically, they've been able to keep a [single logical qubit stable](#) enough so errors occur maybe once every

Fault Tolerant Quantum Computing

Google's New Chip Closes Quantum Computing's Problems

TECH 11 December 2024 By DAVID NIELD



Google's new quantum chip Willow. (Google)

In spite of [the advances made](#) towards making qubit-based systems remain unstable and highly something Google may have taken a major step

Through a newly unveiled quantum chip called Willow, Google has passed a significant milestone in error handling, showing that it can keep a single logical qubit stable enough so errors occur maybe once every



Atom shows record 24 logical qubit quantum computer

Technology News | November 21, 2024

By Nick Flaherty

QUANTUM

Atom Computing in the US and Microsoft have entangled 24 logical qubits, setting a new world record. The two companies have also demonstrated error detection, correction, and computation with 28 logical qubits on Atom's flagship systems.

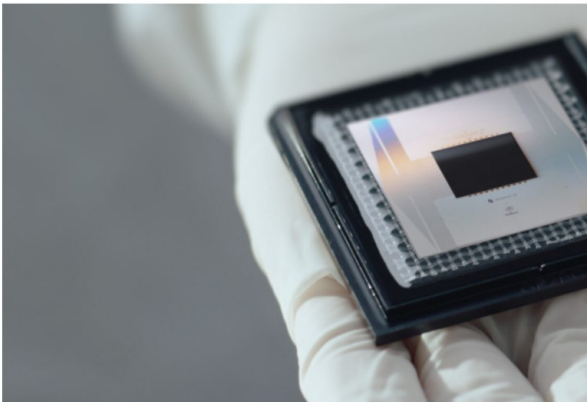
The quantum computer uses neutral Ytterbium (Yb) atoms manipulated with lasers, creating the logical qubits from 112 physical qubits.

This is a key step for fault tolerant quantum computing to solve large computational problems beyond classical computing, and it requires the integration of multiple advanced technologies and quantum error correction algorithms to provide sufficient reliable computing resources

Fault Tolerant Quantum Computing

Google's New Chip Could Solve Quantum Computing's Problems

TECH 11 December 2024 By DAVID NIELD



Google's new quantum chip Willow. (Google)

In spite of [the advances made](#) towards making quantum computing practical, qubit-based systems remain unstable and highly error-prone. Google may have taken a major step

Through a newly unveiled quantum chip called Willow, Google has passed a significant milestone in error handling. The chip is designed to keep a single logical qubit stable enough so errors occur maybe once every



Atom Computing in the US and Microsoft have demonstrated error detection, correction, and logical qubits on Atom's flagship systems.

The quantum computer uses neutral Ytterbium ions, trapped with lasers, creating the logical qubits from

This is a key step for fault tolerant quantum computing, allowing for the integration of multiple advanced technologies

correction algorithms to provide sufficient redundancy to keep a single logical qubit stable enough so errors occur maybe once every

Atom shows record 24 logical qubit

Scientists make 'magic state' breakthrough after 20 years — without it, quantum computers can never be truly useful

News By Keumars Afifi-Sabet published July 17, 2025

Scientists demonstrate a process called "magic state distillation" in logical qubits for the first time, meaning we can now build quantum computers that are both error-free and more powerful than supercomputers.

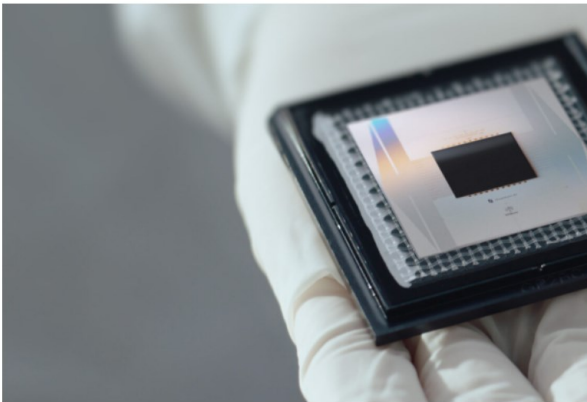
In a world first, scientists have demonstrated an enigmatic phenomenon in [quantum computing](#) that could pave the way for fault-tolerant machines that are far more powerful than any supercomputer.

The process, called "magic state distillation," was first [proposed 20 years ago](#), but its use in logical qubits has eluded scientists ever since. It has long been considered crucial for producing the high-quality resources, known as "magic states," needed to fulfill the full potential of quantum computers.

Fault Tolerant Quantum Computing

Google's New Chip Could Solve Quantum Computing's Problems

TECH 11 December 2024 By DAVID NIELD



Google's new quantum chip Willow. (Google)

In spite of [the advances made](#) towards making quantum computing practical, qubit-based systems remain unstable and highly error-prone. Google may have taken a major step

Through a newly unveiled quantum chip called Willow, Google has passed a significant milestone in error handling. The chip is designed to keep a single logical qubit stable enough so errors occur maybe once every



Atom Computing in the US and Microsoft have demonstrated error detection, correction, and logical qubits on Atom's flagship systems.

The quantum computer uses neutral Ytterbium ions, trapped with lasers, creating the logical qubits from

This is a key step for fault tolerant quantum computing, allowing for the integration of multiple advanced technologies

correction algorithms to provide sufficient redundancy to keep a single logical qubit stable enough so errors occur maybe once every

Atom shows record 24 logical qubit

Scientists make 'magic state' breakthrough after 20 years — without it, quantum computers can never be truly useful

By



News

By Keumars Afifi-Sabet published July 17, 2025

Scientists demonstrate a process called "magic state distillation" in logical qubits for the first time, meaning we can now build quantum computers that are both error-free and more powerful than supercomputers.

In a world first, scientists have demonstrated an enigmatic phenomenon in quantum computing that could pave the way for fault-tolerant machines that are far more powerful than any supercomputer.

The process, called "magic state distillation," was first [proposed 20 years ago](#), but its use in logical qubits has eluded scientists ever since. It has long been considered crucial for producing the high-quality resources, known as "magic states," needed to fulfill the full potential of quantum computers.

Roadmaps

Roadmaps

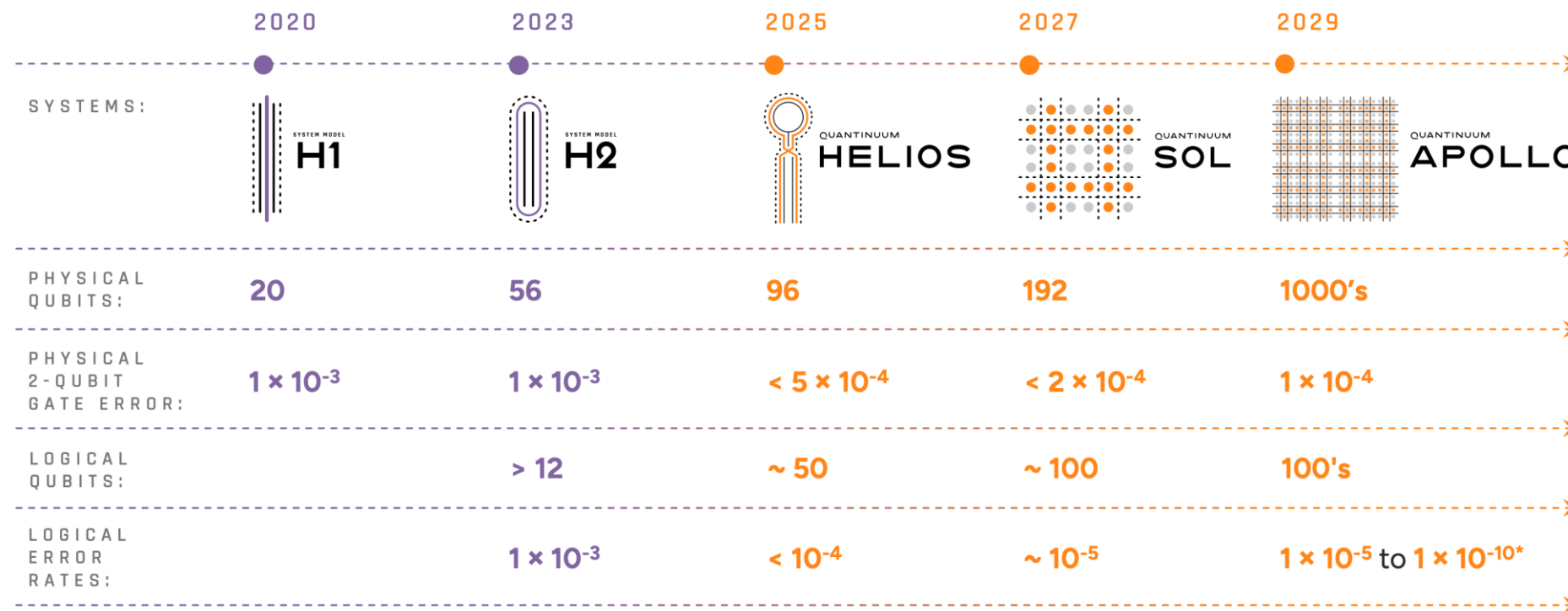
Development Roadmap

IBM Quantum

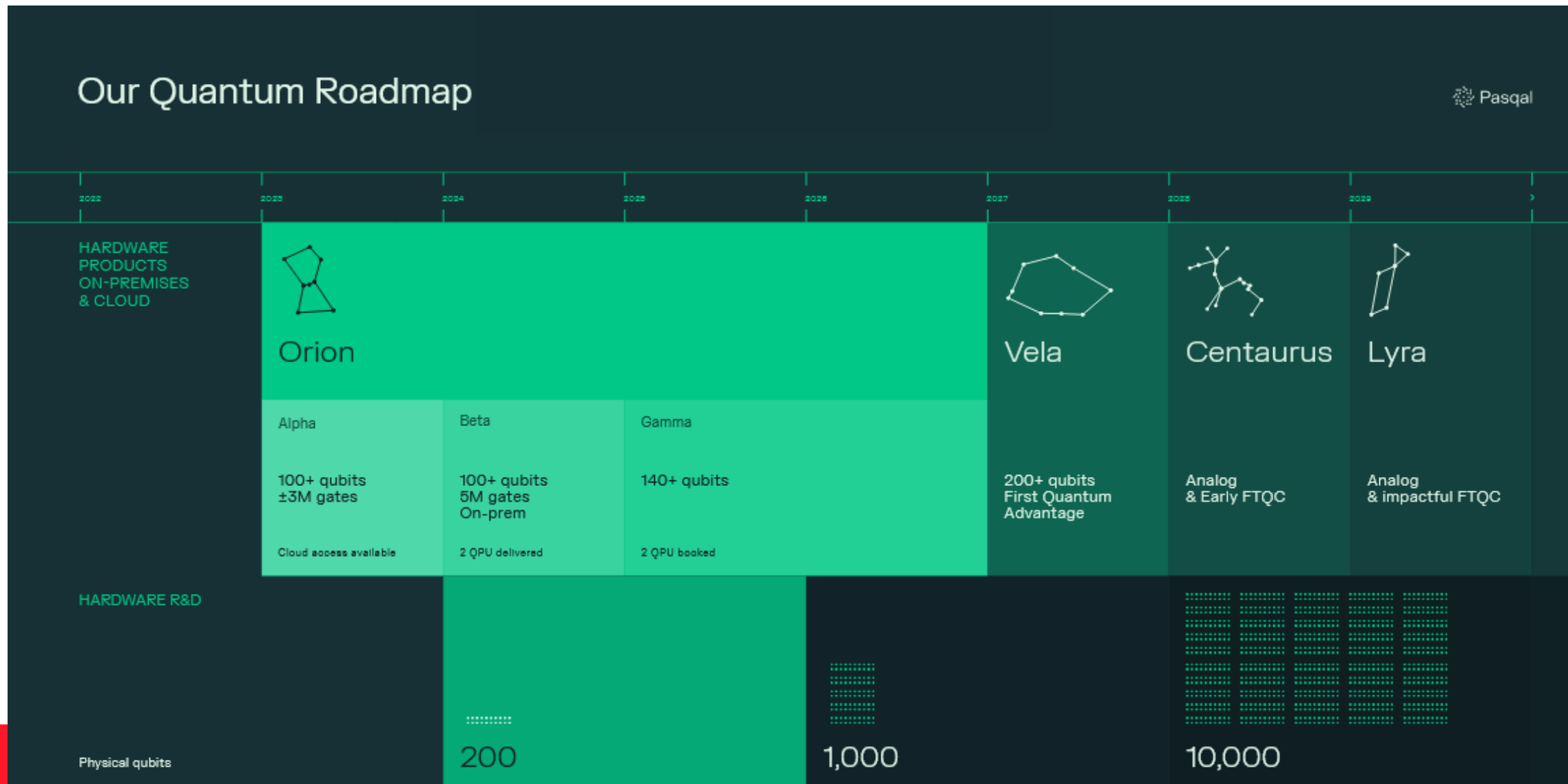
	2016–2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2033+
	Run quantum circuits on the IBM Quantum Platform	Release multi-dimensional roadmap publicly with initial aim focused on scaling	Enhancing quantum execution speed by 100x with Qiskit Runtime	Bring dynamic circuits to unlock more computations	Enhancing quantum execution speed by 5x with quantum serverless and Execution modes	Improving quantum circuit quality and speed to allow 5K gates with parametric circuits	Enhancing quantum execution speed and parallelization with partitioning and quantum modularity	Improving quantum circuit quality to allow 7.5K gates	Improving quantum circuit quality to allow 10K gates	Improving quantum circuit quality to allow 15K gates	Improving quantum circuit quality to allow 100M gates	Beyond 2033, quantum-centric supercomputers will include 1000's of logical qubits unlocking the full power of quantum computing
Data Scientist						Platform						
						Code assistant	Functions	Mapping Collection	Specific Libraries			General purpose QC libraries
Researchers					Middleware							
					Quantum Serverless	Transpiler Service	Resource Management	Circuit Knitting x P	Intelligent Orchestration			Circuit libraries
Quantum Physicist			Qiskit Runtime									
	IBM Quantum Experience		QASM3	Dynamic circuits	Execution Modes	Heron (5K)	Flamingo (5K)	Flamingo (7.5K)	Flamingo (10K)	Flamingo (15K)	Starling (100M)	Blue Jay (1B)
	Early	Falcon		Eagle		Error Mitigation	Error Mitigation	Error Mitigation	Error Mitigation	Error Mitigation	Error correction	Error correction
	Canary 5 qubits Albatross 16 qubits Penguin 20 qubits Prototype 53 qubits	Benchmarking 27 qubits		Benchmarking 127 qubits		5k gates 133 qubits Classical modular 133x3 = 399 qubits	5k gates 156 qubits Quantum modular 156x7 = 1092 qubits	7.5k gates 156 qubits Quantum modular 156x7 = 1092 qubits	10k gates 156 qubits Quantum modular 156x7 = 1092 qubits	15k gates 156 qubits Quantum modular 156x7 = 1092 qubits	100M gates 200 qubits Error corrected modularity	1B gates 2000 qubits Error corrected modularity

Roadmaps

Development roadmap



Roadmaps



Resource Requirements

Resource Requirements

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

Craig Gidney¹ and Martin Ekerå²

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

²KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3} , a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Van Meter et al. 2009, Jones et al. 2010, Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n -bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

[quant-ph] 13 Apr 2021

Resource Requirements

How to factor 2048 bit RSA integ 20 million noisy qubits

Craig Gidney¹ and Martin Ekerå²

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

²KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

We significantly reduce the cost of factoring integer arithms in finite fields on a quantum computer by co 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ek Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We est our construction using plausible physical assumptions f qubit platforms: a planar grid of qubits with nearest-ne teristic physical gate error rate of 10^{-3} , a surface code cy a reaction time of 10 microseconds. We account for fac such as noise, the need to make repeated attempts, an computation. When factoring 2048 bit RSA integers, ou ume is a hundredfold less than comparable estimates fro al. 2009, Jones et al. 2010, Fowler et al. 2012, Gheorghi circuit model (which ignores overheads from distillation, our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3: 500n^2 + n^2 \lg n$ measurement depth to factor n -bit RSA i topographic implications of our work, both for RSA and f in finite fields.

[quant-ph] 13 Apr 2021

[quant-ph] 21 May 2025

How to factor 2048 bit RSA integers with less than a million noisy qubits

Craig Gidney

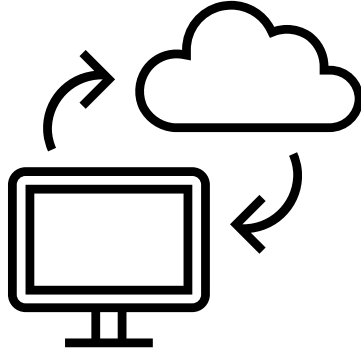
Google Quantum AI, Santa Barbara, California 93117, USA

June 9, 2025

Planning the transition to quantum-safe cryptosystems requires understanding the cost of quantum attacks on vulnerable cryptosystems. In Gidney+Ekerå 2019, I co-published an estimate stating that 2048 bit RSA integers could be factored in eight hours by a quantum computer with 20 million noisy qubits. In this paper, I substantially reduce the number of qubits required. I estimate that a 2048 bit RSA integer could be factored in less than a week by a quantum computer with less than a million noisy qubits. I make the same assumptions as in 2019: a square grid of qubits with nearest neighbor connections, a uniform gate error rate of 0.1%, a surface code cycle time of 1 microsecond, and a control system reaction time of 10 microseconds.

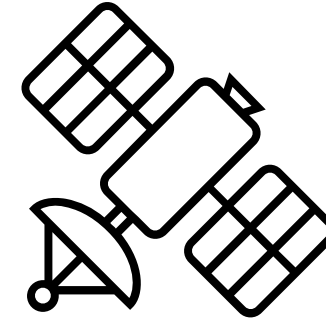
The qubit count reduction comes mainly from using approximate residue arithmetic (Chevignard+Fouque+Schrottenloher 2024), from storing idle logical qubits with yoked surface codes (Gidney+Newman+Brooks+Jones 2023), and from allocating less space to magic state distillation by using magic state cultivation (Gidney+Shutty+Jones 2024). The longer runtime is mainly due to performing more Toffoli gates and using fewer magic state factories compared to Gidney+Ekerå 2019. That said, I reduce the Toffoli count by over 100x compared to Chevignard+Fouque+Schrottenloher 2024.

Quantum and Cybersecurity



Post-Quantum Cryptography (PQC)

- Use alternate **classical encryption** techniques to protect classical data **against quantum attacks**.
- NIST post quantum cryptography standards (<https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>)
- Potentially vulnerable if new quantum or classical algorithms are developed.



Quantum Key Distribution (QKD)

- Use **quantum communication** techniques to distribute a private one-time pad.
- **Information theoretically** secure.
- Requires **new hardware** installed at each point of communication.
- Can be **device dependent** (secure if you trust the distributor) or **device-independent** (security even with untrusted distributor).

More Quantum Primitives

- Certified Randomness from Quantum Devices.
 - Achievable with current quantum hardware.
 - If you trust the device: low-cost, high-rate options. **No quantum computer required.**
 - Quantum computers can generate device-independent certified randomness.
- Quantum Networks\Quantum Internet.
 - Connecting quantum computers with quantum communication may allow for classically impossible cryptographic primitives.
 - Requires large quantum computers with quantum networks between them.
 - Unforgeable quantum money.
 - Quantum secret sharing.
 - Homomorphic (blind) quantum computation

Thanks! Questions?

.....

Adam Bene Watts
Adam.benewatts@ucalgary.ca



**Quantum
City**



qConnect 2025: November 5-6, 2025



qConnect 2025 is the premier industry event for quantum technology, bringing together businesses, tech creators, startups, government and investors to transform ideas into impact.