BlueHat IL

2026

The Sooner Organizations Start their Quantum-Safe Transformation the Safer They Will Be.

Systems are vulnerable already today:

1. Encrypted data can be recorded and stored today to be decrypted in the future (harvest now, decrypt later)
2. Hard-to-update systems with long deployment lifetimes

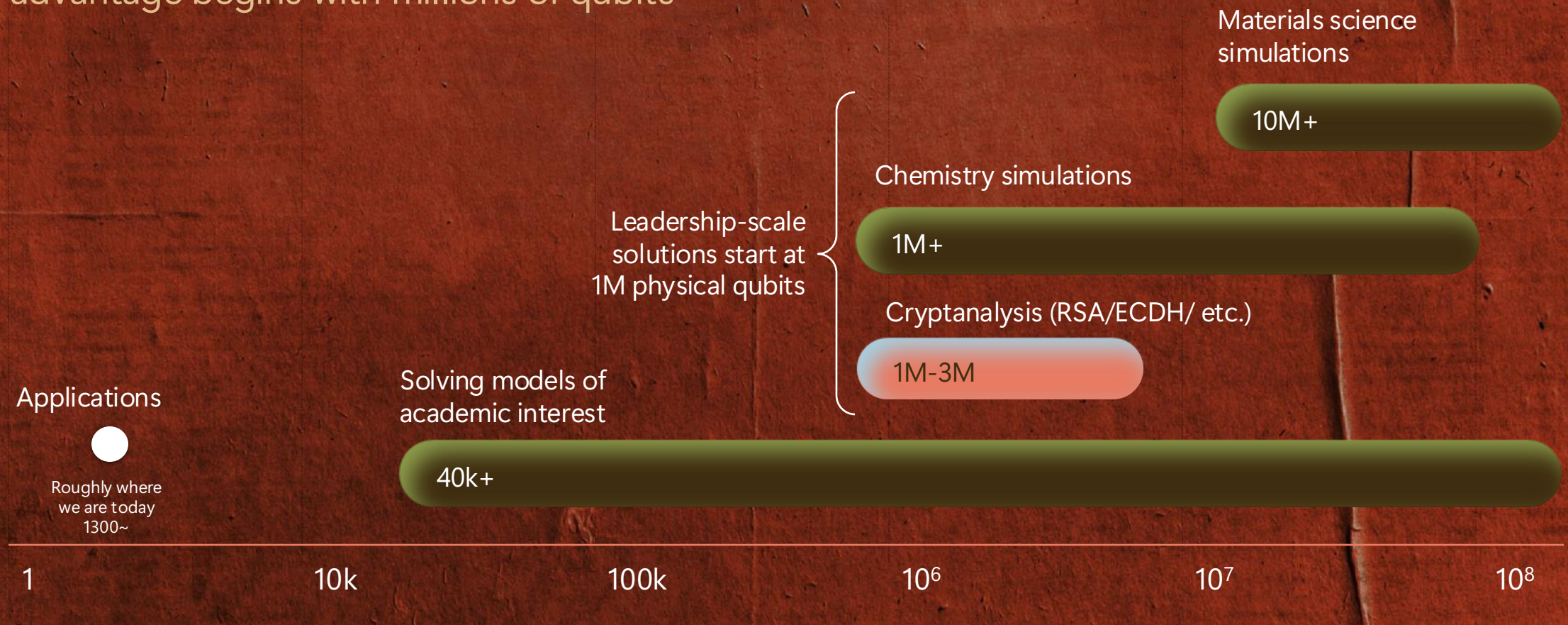
Multi-year and complex transition:

1. The scale of reaching quantum-safety is pervasive, spanning multiple security layers.
2. Inventorying and updating all asymmetric cryptography usage is a complex and expensive process

BlueHat IL

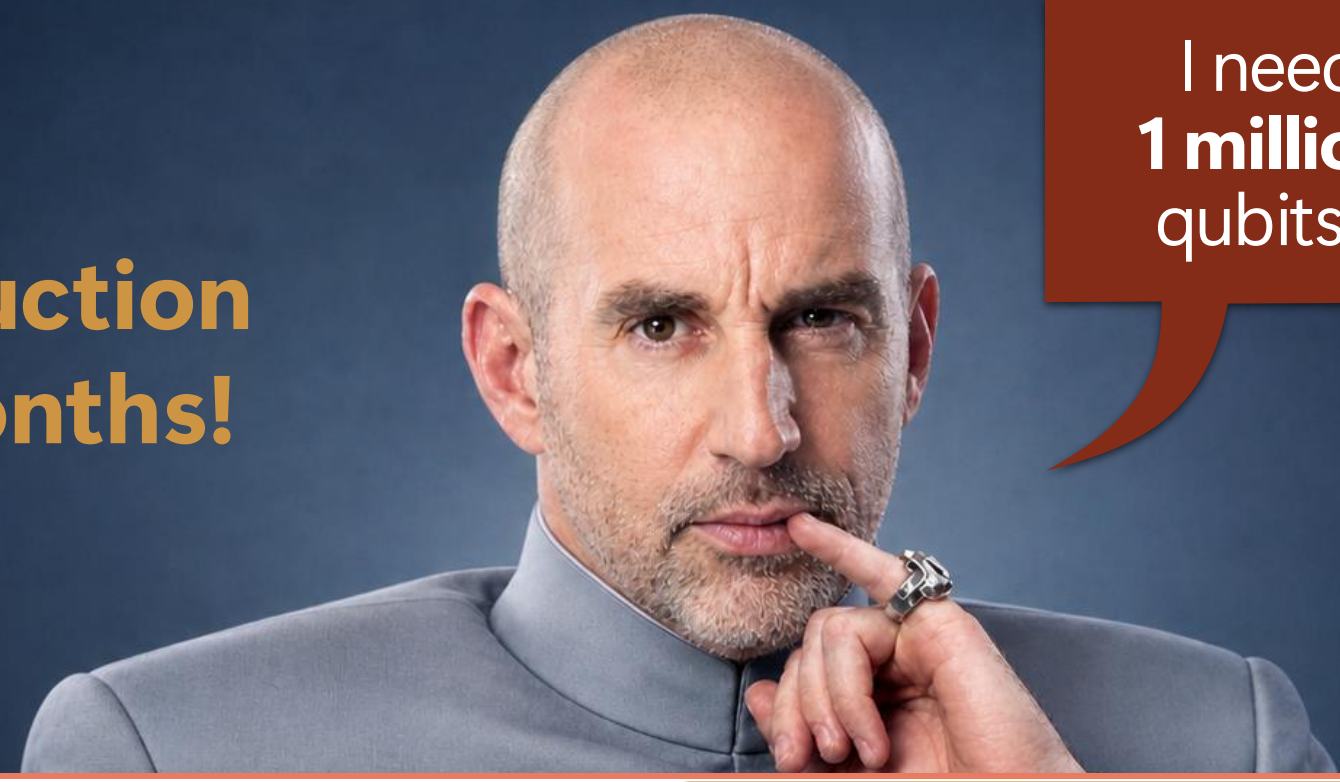
Modern Cryptography - Understanding the Hype Vs. Reality

Today's quantum computers do not pose a legitimate threat - Practical quantum advantage begins with millions of qubits



BlueHat IL

x100 Reduction in ~14 Months!



Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits

Madelyn Cain[1,*,†], Qian Xu[1,2,*,‡], Robbie King[1], Lewis R. B. Picard[1], Harry Levine[1,3], Manuel Endres[1,2], John Preskill[1,2], Hsin-Yuan Huang[1,2], Dolev Bluvstein[1,2,§]

[1] *Oratomic, Pasadena, California 91125, USA*

[2] *California Institute of Technology, Pasadena, California 91125, USA*

[3] *Department of Physics, University of California, Berkeley, California 94720, USA*

[†] *mcain@oratomic.com*, [‡] *qxu@oratomic.com*, [§] *dbluvstein@oratomic.com*

[*] *These authors contributed equally*

(Dated: March 31, 2026)

BLUEHAT IL

Quantum-Safe Solutions Available Today

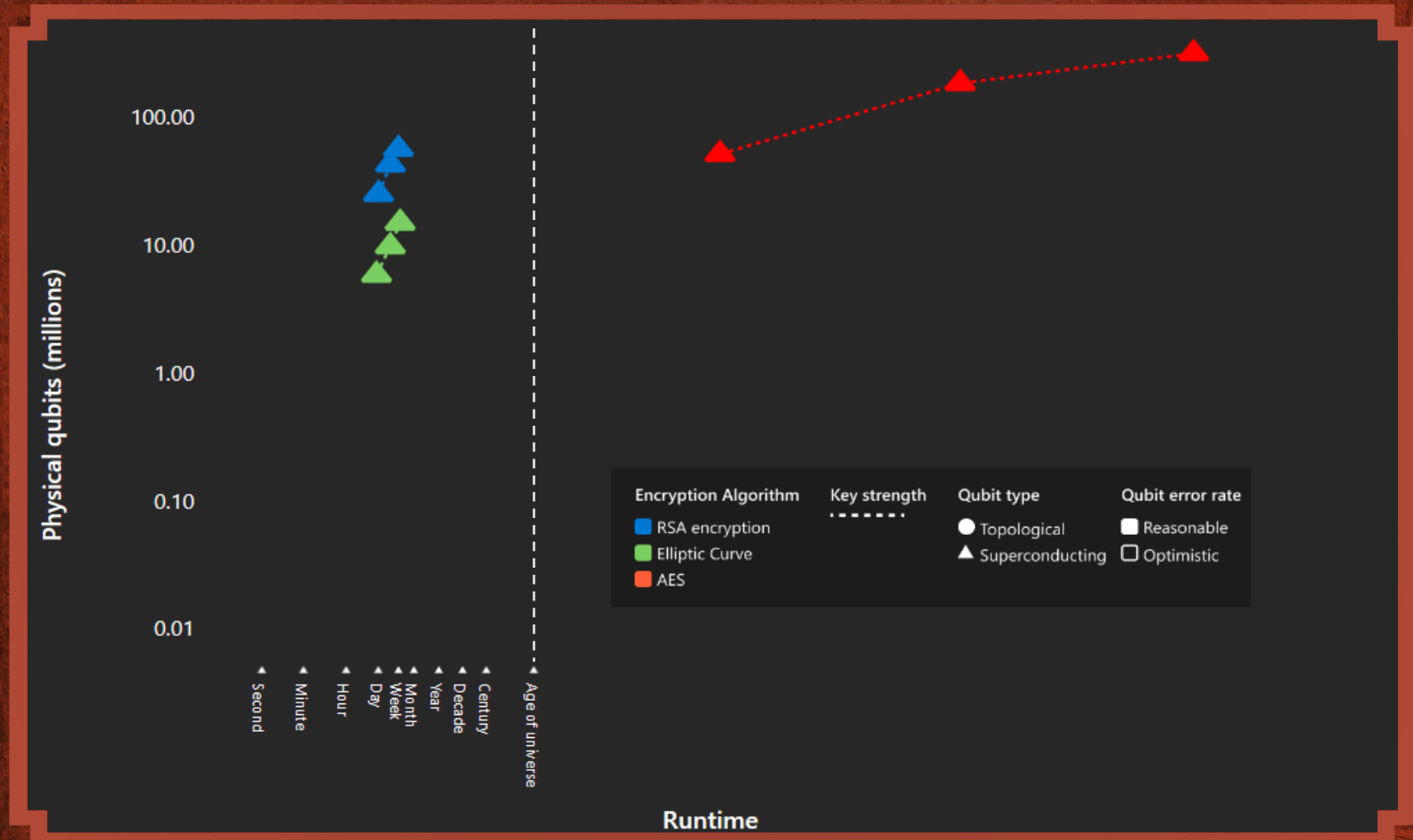
Symmetric Encryption and Post-Quantum Cryptography (PQC)

Symmetric encryption could be considered quantum-safe

PQC are new asymmetric algorithms

BlueHat IL

The Future Risk to Symmetric Encryption Vs. Asymmetric Encryption



Captured from the Azure Quantum Resource Estimator.

BlueHat IL


QUANTUM COMPUTING
It's Not Ten Years Away
Dr. Tomer Simon
Partner Chief Scientist, Microsoft Security
Microsoft

"Everything we call real is made of things that cannot be regarded as real"

Niels Bohr

"If quantum theory is correct, it signifies the end of physics as a science"

Albert Einstein

"Quantum mechanics makes absolutely no sense"

Roger Penrose

"It is safe to say that nobody understands quantum mechanics"

Richard Feynman

"I do not like quantum mechanics, and I am sorry I ever had anything to do with it"

Erwin Schrödinger

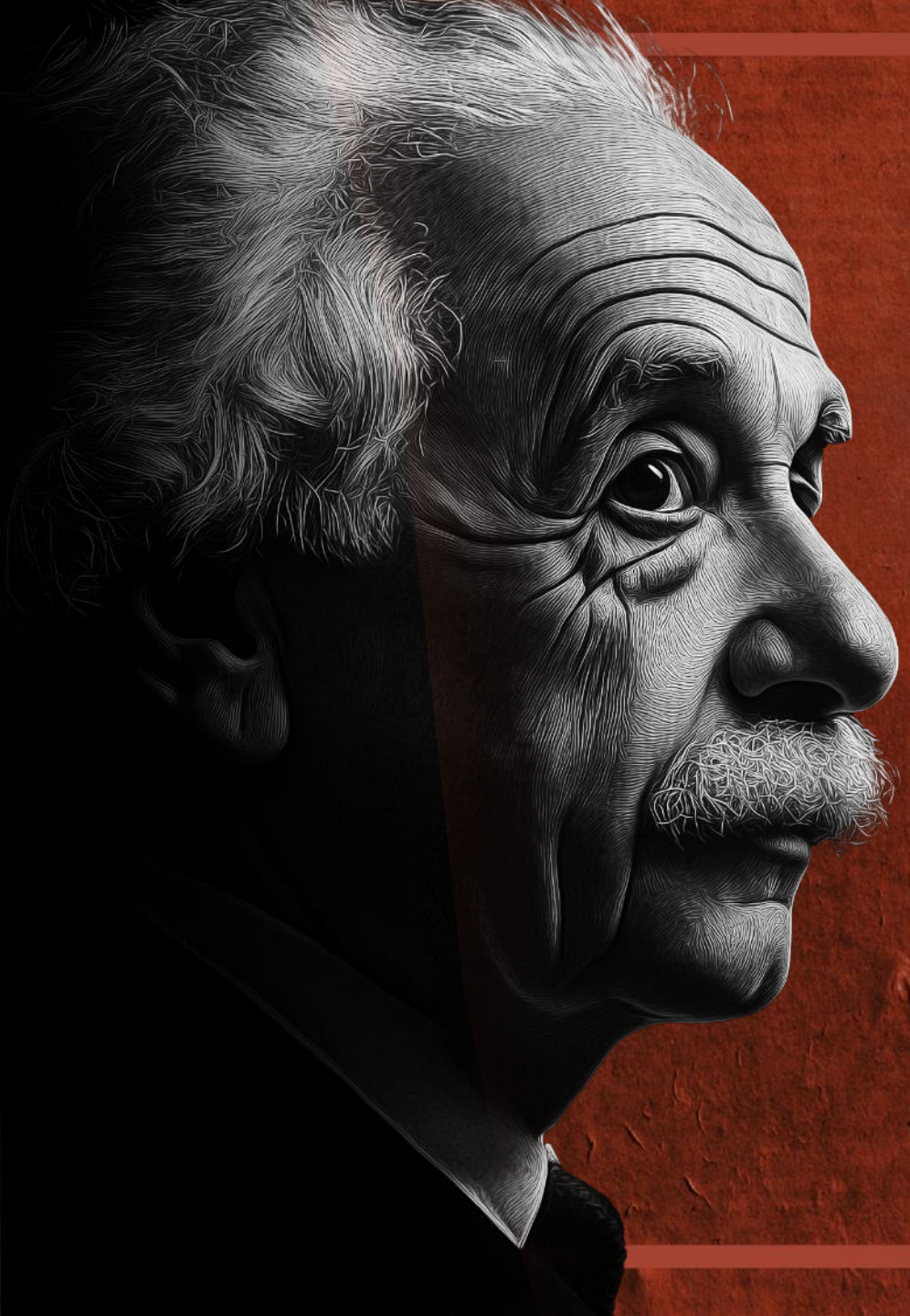
"Those who are not shocked when they first come across quantum theory cannot possibly have understood it"

Niels Bohr

"If you are not completely confused by quantum mechanics, you do not understand it"

John Wheeler

BLUEHAT IL



If You Can't Explain it Simply, You **Don't Understand** it Well Enough.

Albert Einstein

BlueHat IL


BlueHat IL

Harvard Business Review

Latest Magazine Popular Topics Podcasts Video Store The Big Idea

TECHNOLOGY

Are You Ready for th Quantum Computin Revolution?

by Sh

Septem

MIT Technology Review

Topics Magazine Newsletters Events

Computing / Quantum computing

et News

Wave Quantum Surfs to ccess With Quantum eakthrough and Strong nancials

Ran Melamed
Mar 16, 2025, 03:39 PM

A+ A-

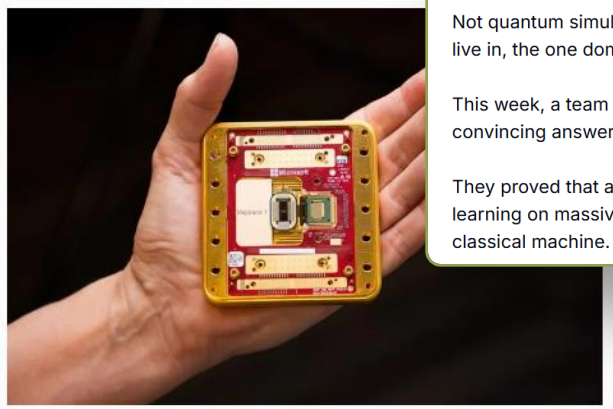
Subscribe To Newsletters

Massive Microsoft Quantu Breakthrough Uses New S

By John Koetsier , Senior Contributor. Journalist, analyst, author, podcaster

Feb 19, 2025, 11:04am EST

Share Save Comment 1



Microsoft's new Majorana 1 quantum computing chip JOHN BRECHER

ZDN

Quan them

By Daphne Lep

to quantum computing

Quantum Computers Are Finally Doing Something Useful

Exponential quantum advantage on real-world AI tasks

Michaela Eichinger
Apr 12, 2026

Hey!

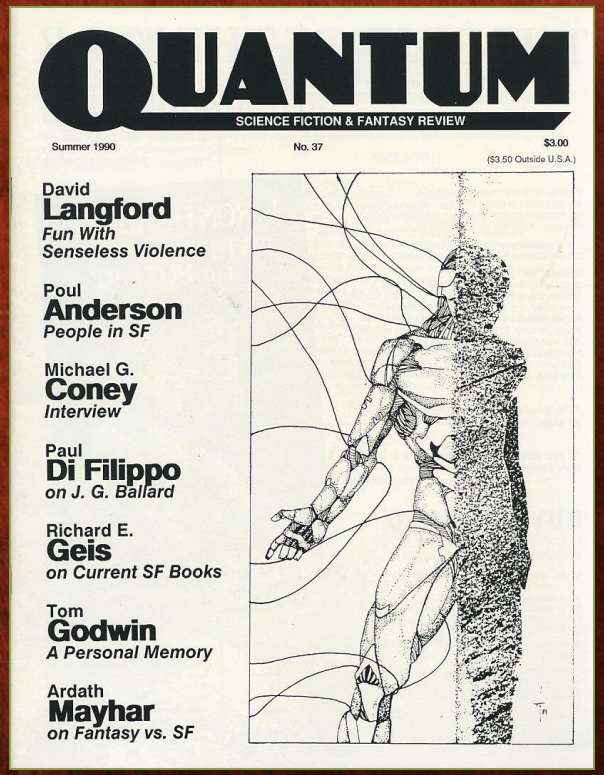
For years, the most common and frankly most reasonable critique of quantum computing has been: "When will it do something useful on real-world problems?"

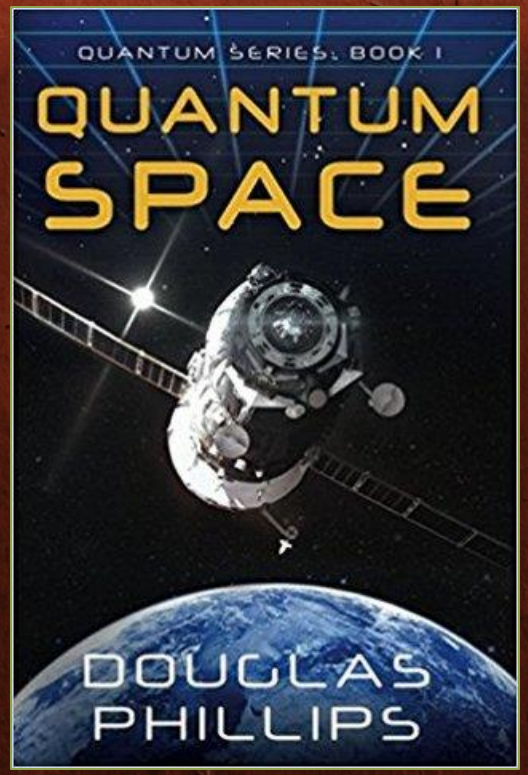
Not quantum simulation. Not breaking encryption. Something that actually matters for the world we live in, the one dominated by classical data, classical machine learning, and classical AI.

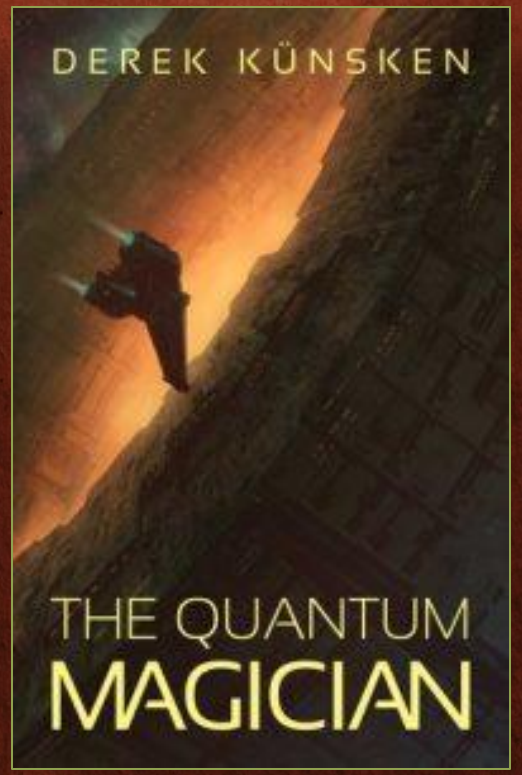
This week, a team from Caltech, Google Quantum AI, MIT, and Oratomic published the most convincing answer yet!

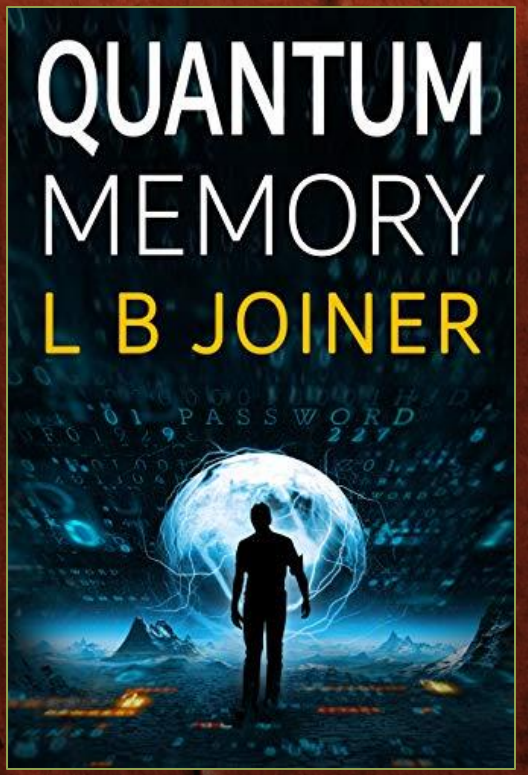
They proved that a quantum computer with fewer than 60 logical qubits can perform machine learning on massive classical datasets using ten thousand to a million times less memory than any classical machine.

BlueHat IL


QUANTUM
SCIENCE FICTION & FANTASY REVIEW
Summer 1990
No. 37
$3.00
($3.50 Outside U.S.A.)
David
Langford
Fun With
Senseless Violence
Poul
Anderson
People in SF
Michael G.
Coney
Interview
Paul
Di Filippo
on J. G. Ballard
Richard E.
Geis
on Current SF Books
Tom
Godwin
A Personal Memory
Ardath
Mayhar
on Fantasy vs. SF


QUANTUM SERIES: BOOK 1
QUANTUM SPACE
DOUGLAS PHILLIPS


DEREK KÜNSKEN
THE QUANTUM MAGICIAN

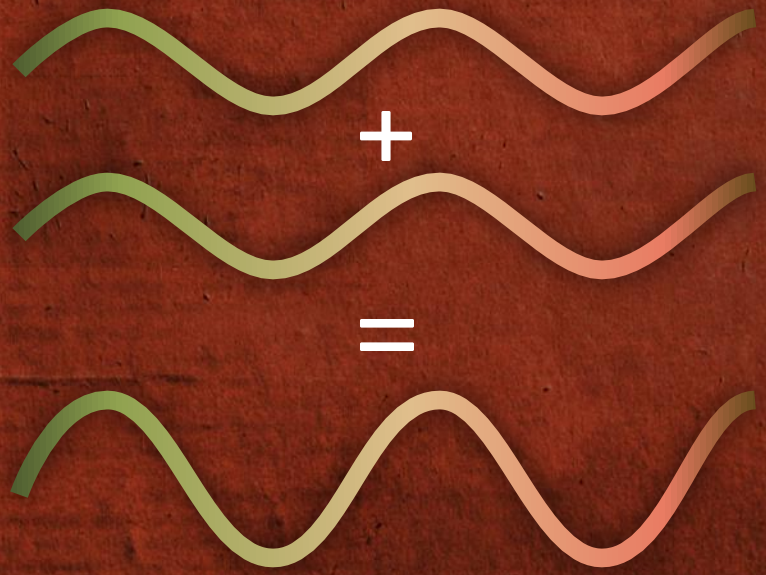

QUANTUM MEMORY
L B JOINER


BLUEHAT IL

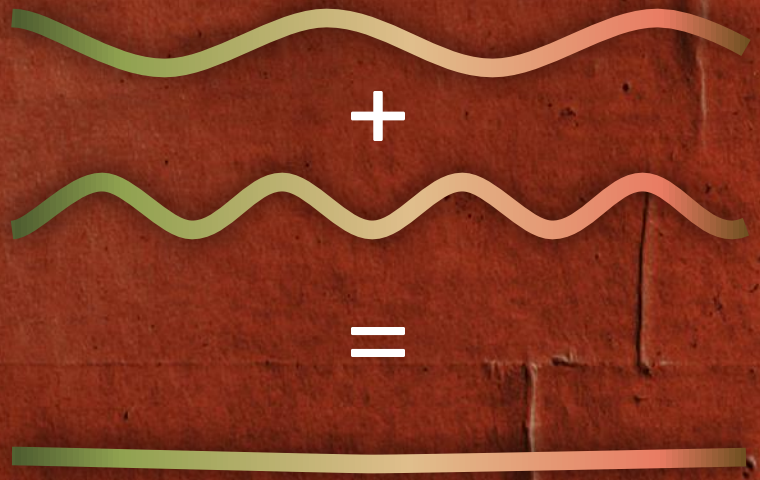
Light Waves

Light Particles

BlueHat IL

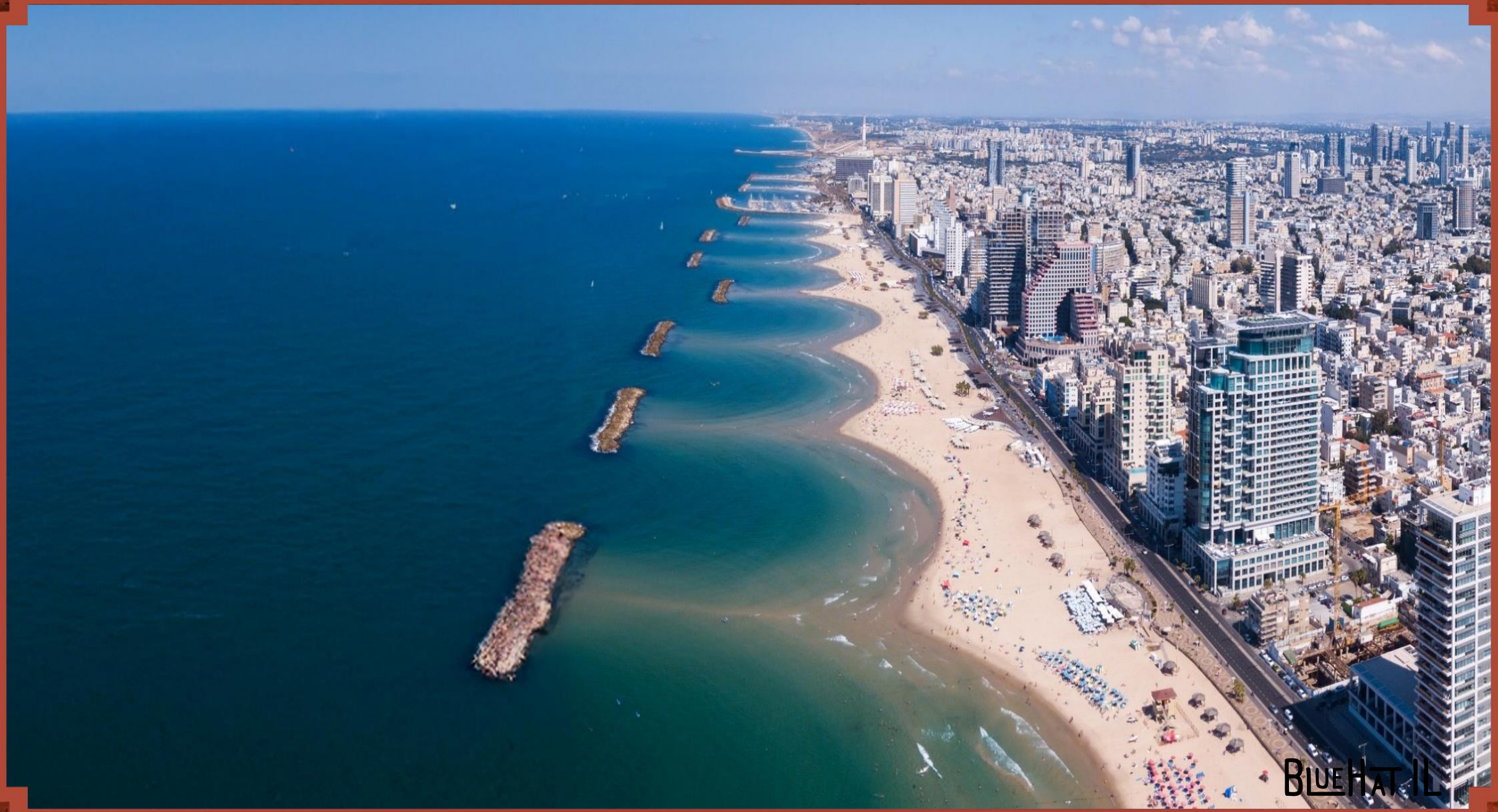


Constructive Interference

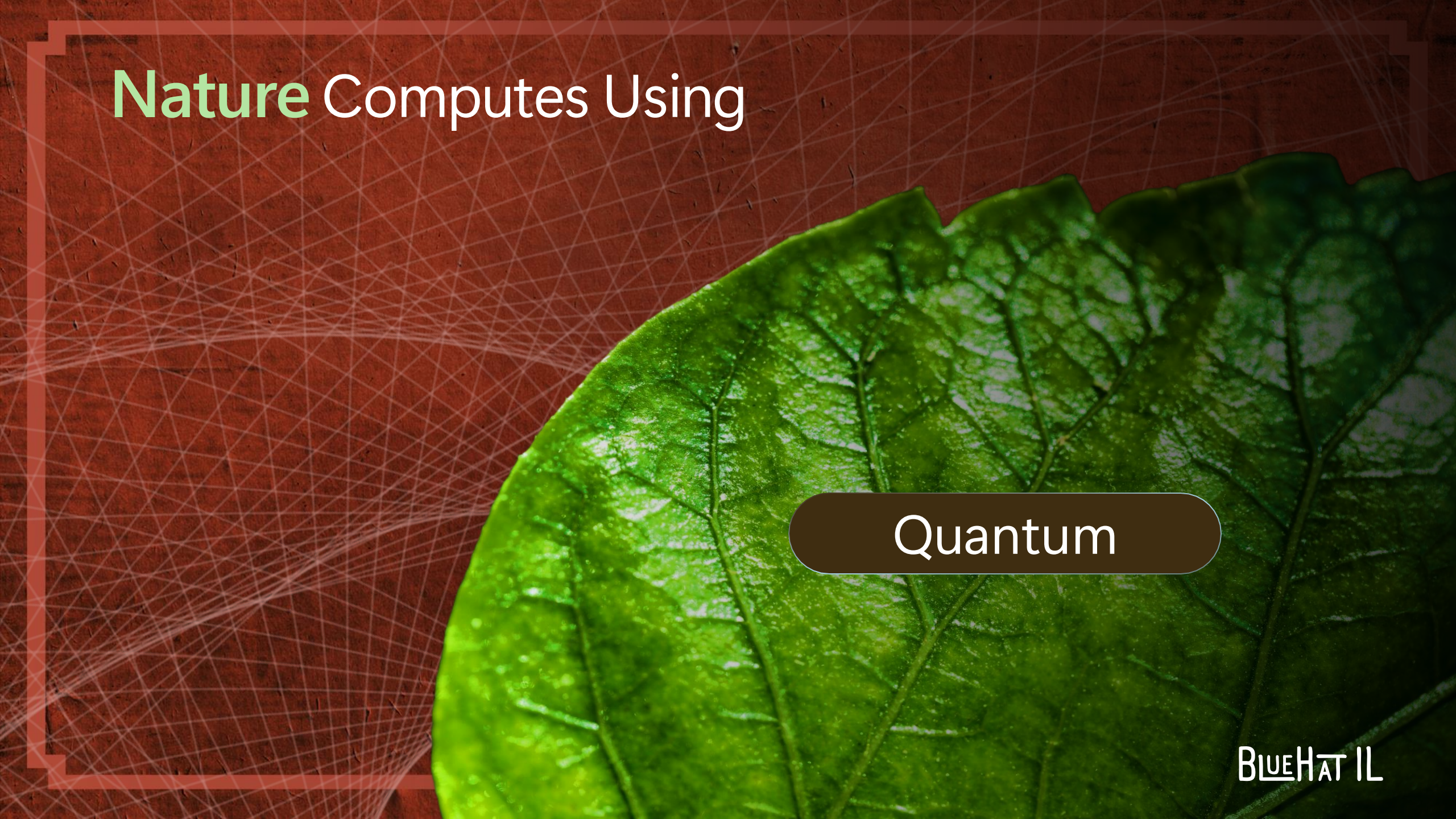


Destructive Interference

BlueHat IL

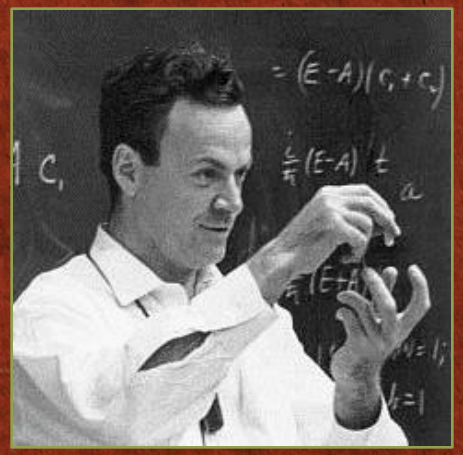

BlueHat IL

Nature Computes Using



BlueHat IL

History of Quantum Computing



"I think I can safely say that nobody understands quantum mechanics"

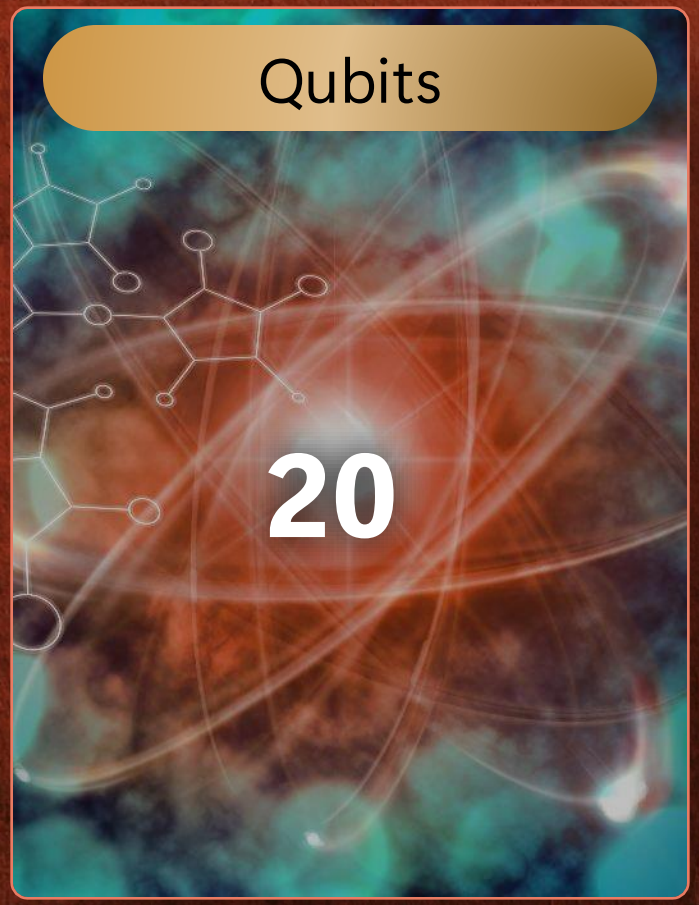
Richard Feynman

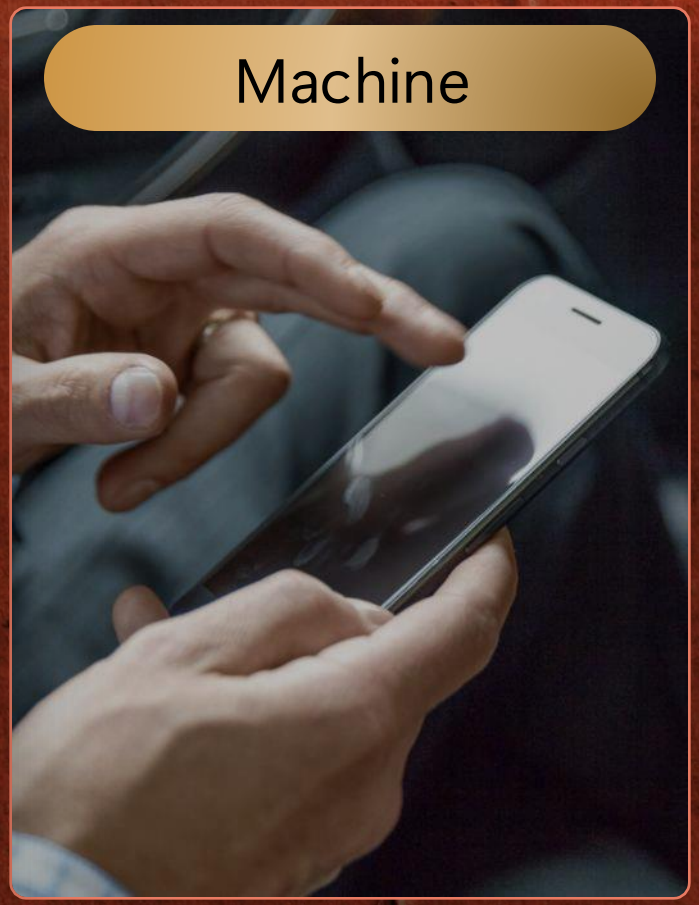
BlueHat IL

From Bit to Qubit

BlueHat IL

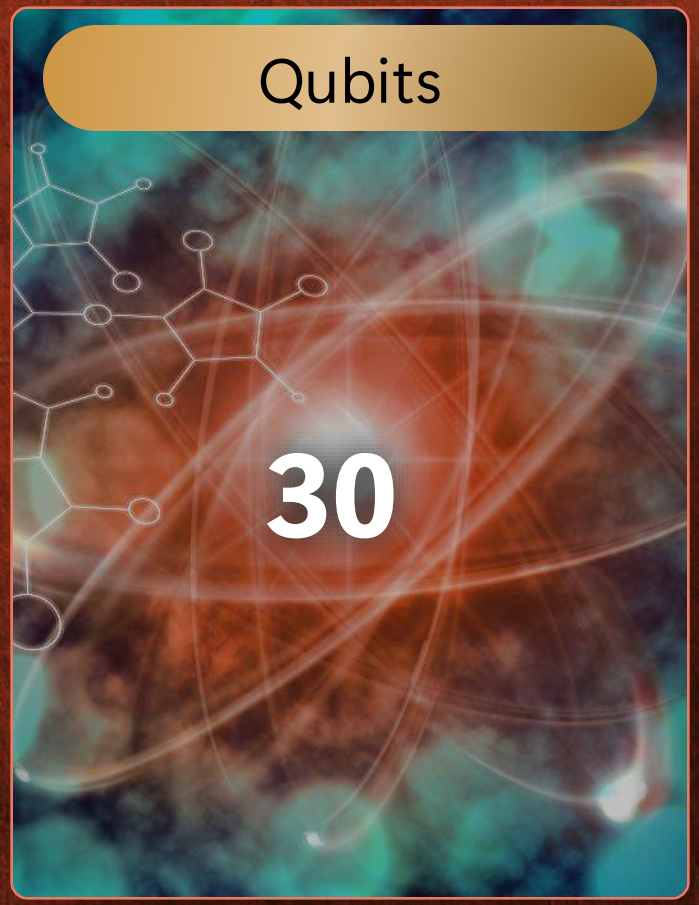
Simulating Quantum Computers on Classical Computers

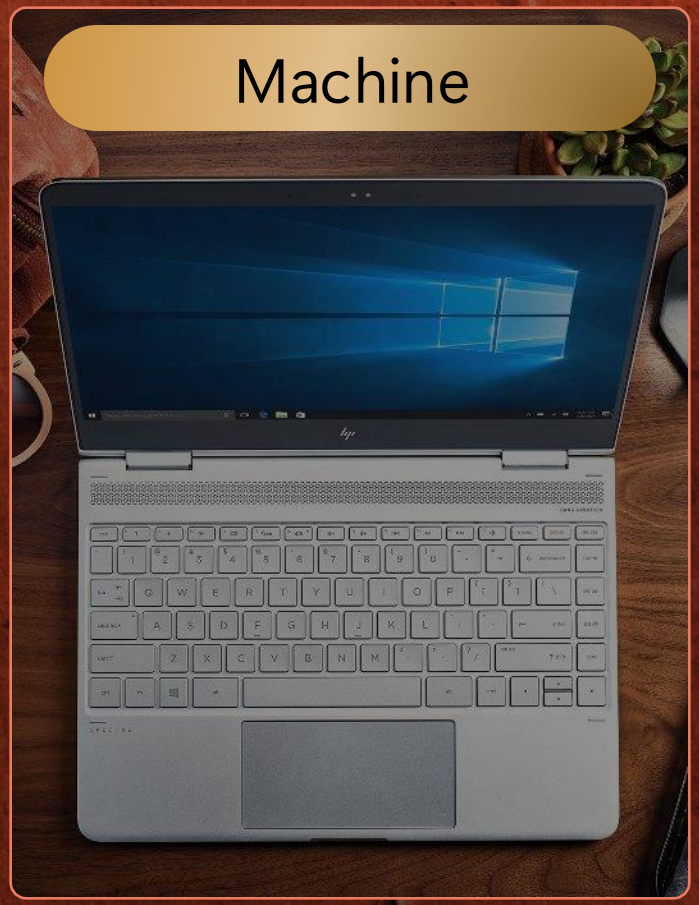




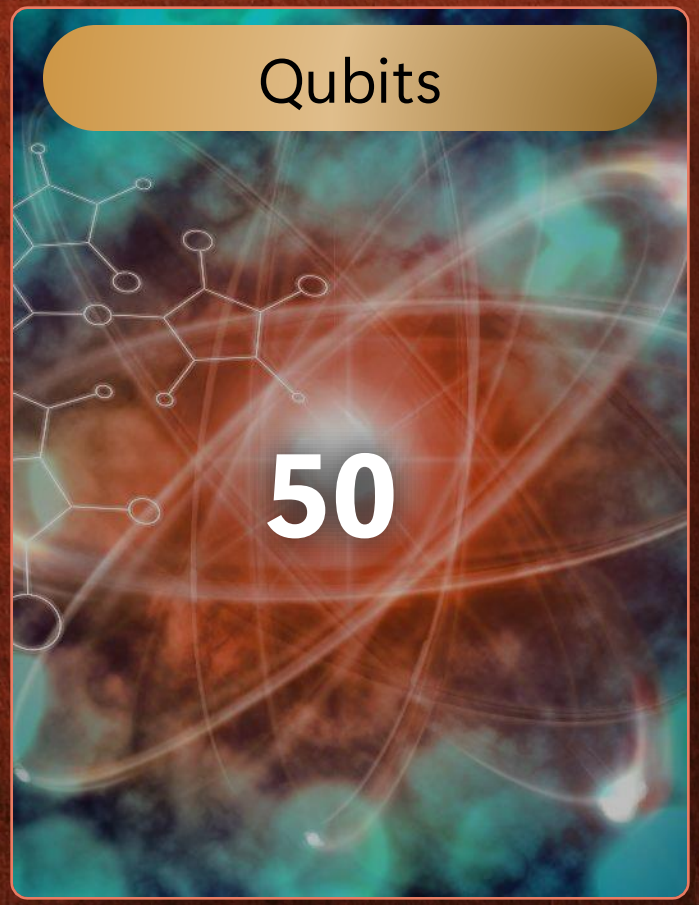
BlueHat IL

Simulating Quantum Computers on Classical Computers

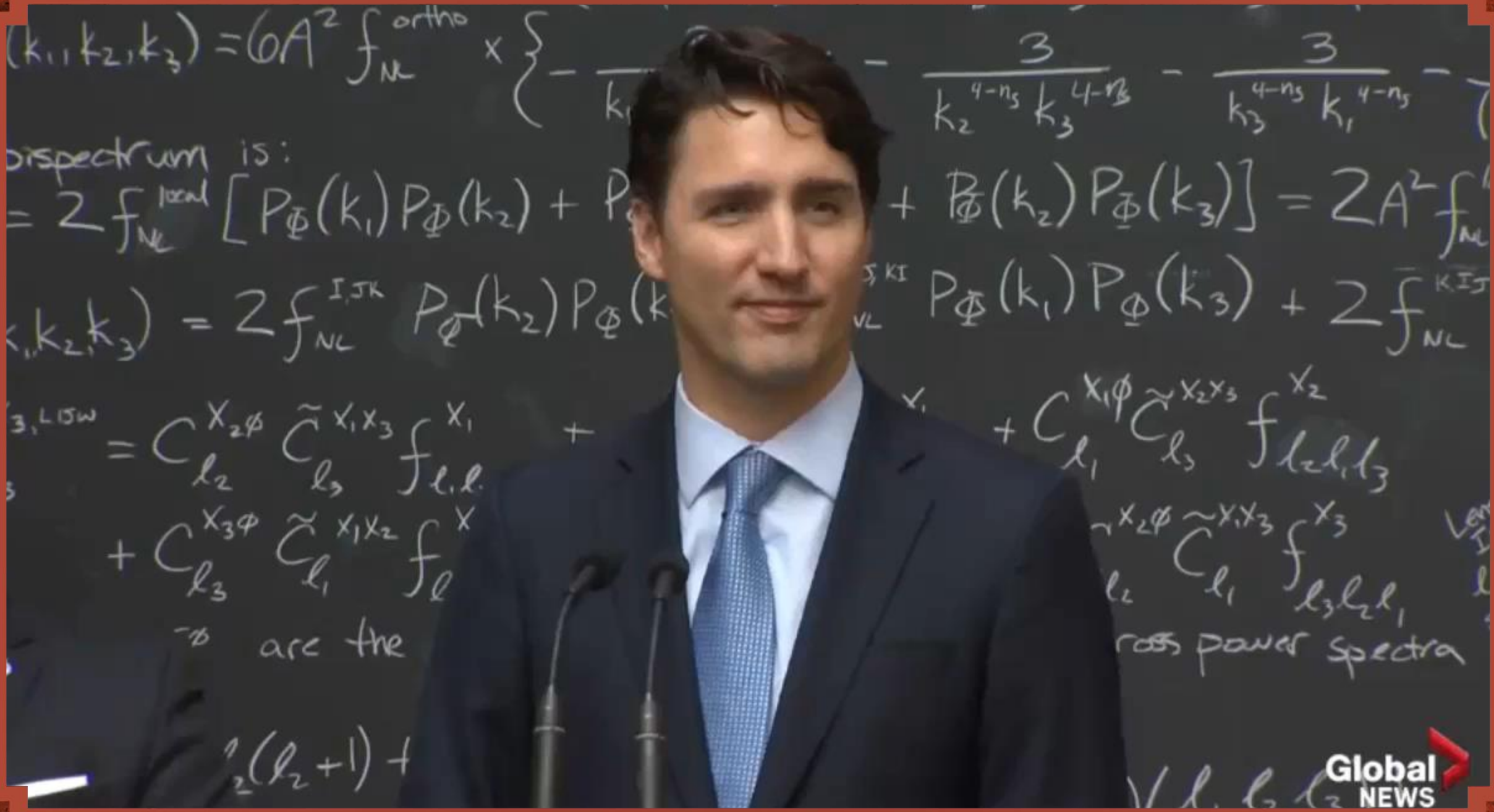




Simulating Quantum Computers on Classical Computers



BlueHat IL


Global
NEWS


Schrödinger's
CAT
$\Delta x \Delta p \geq \frac{\hbar}{2}$
BlueHat IL

Schrödinger Plates

They’re both broken and not broken until you open the door

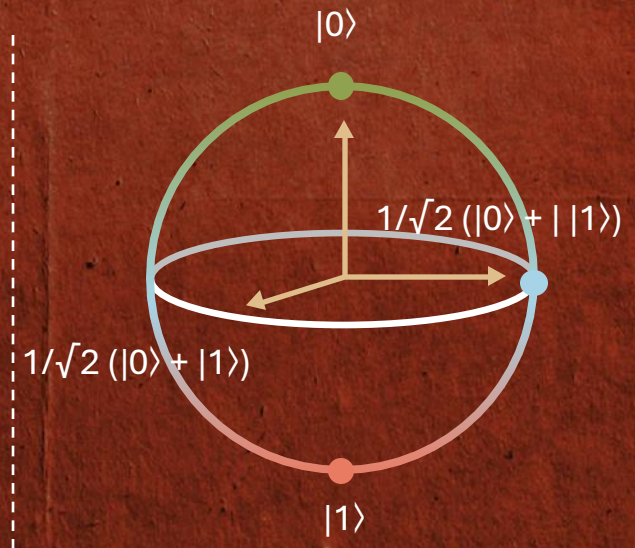
BlueHat IL

Why is Quantum Different?

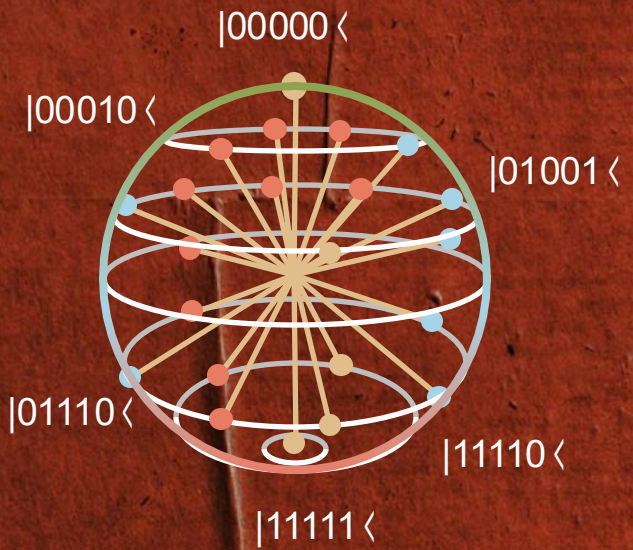
```
Qubit q = Zero;
Q = One;
float a, b;
Q = a * Zero + b * One;
```

FALSE / OFF BITS TRUE / ON

Classical states



Bloch Sphere (1 Qubit)



Qsphere (5 Qubits)

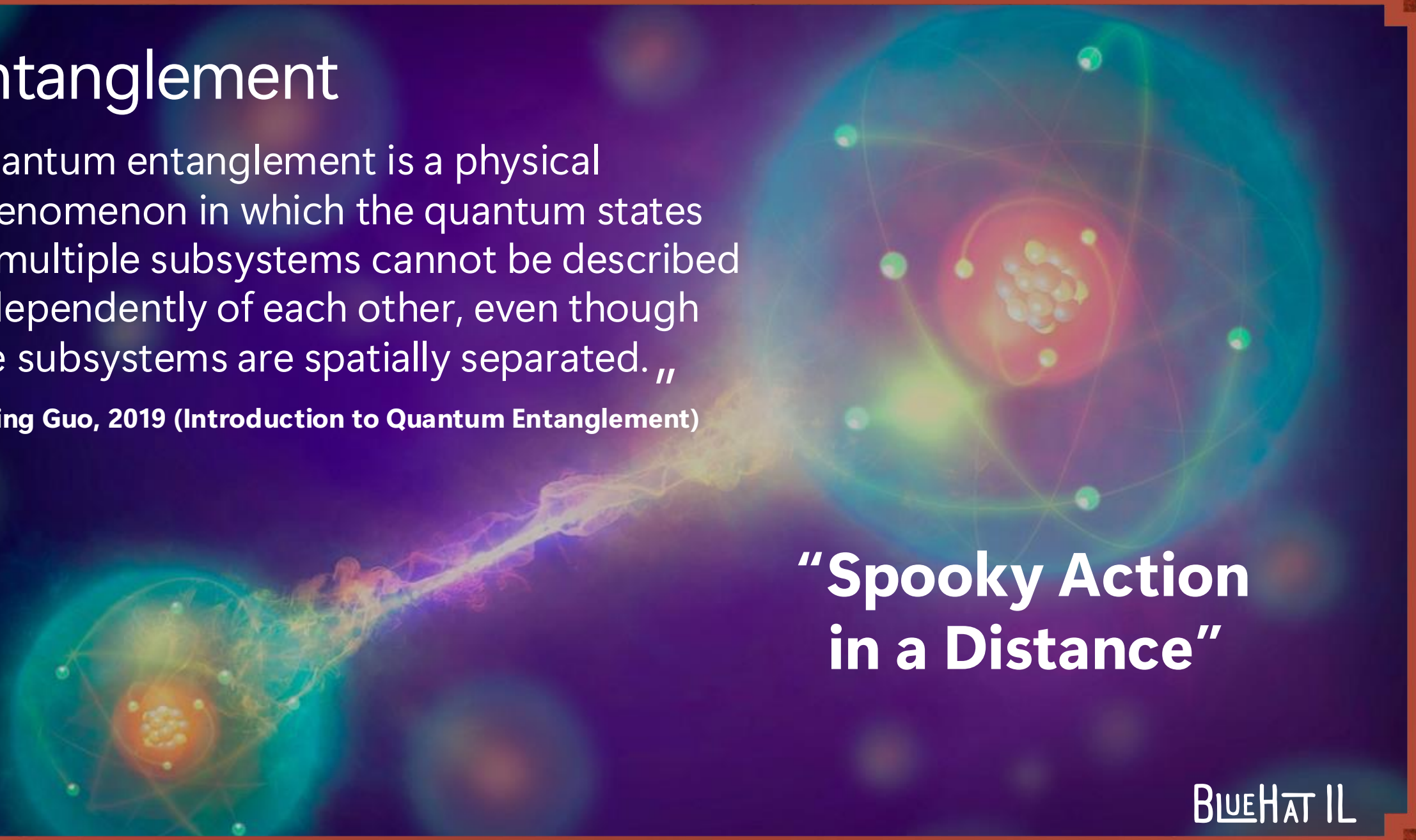
Quantum states

BlueHat IL

Entanglement

" Quantum entanglement is a physical phenomenon in which the quantum states of multiple subsystems cannot be described independently of each other, even though the subsystems are spatially separated. "

Yuying Guo, 2019 (Introduction to Quantum Entanglement)



"Spooky Action in a Distance"

BlueHat IL

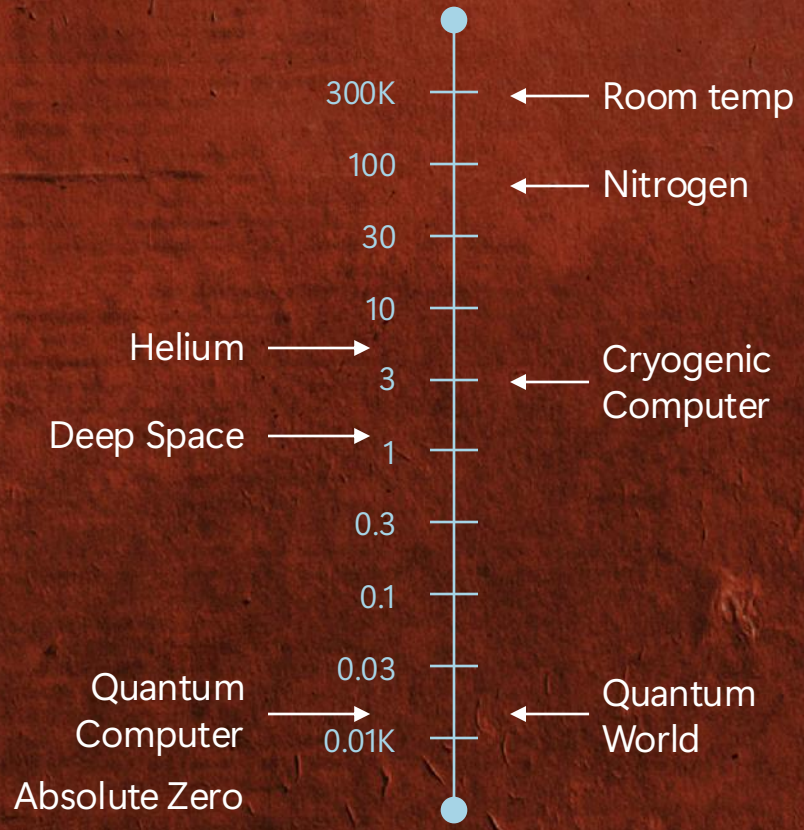
"Nature Isn't Classical, Dammit, and if You Want to Make a Simulation of Nature, You'd Better Make it Quantum Mechanical, and by Golly it's a Wonderful Problem, Because it Doesn't Look So Easy."

Richard Feynman

BlueHat IL


The **Quantum**
Computer!
BlueHat IL

A Complete, Scalable, **Quantum System**

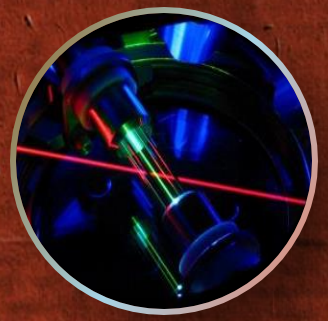


BlueHat IL

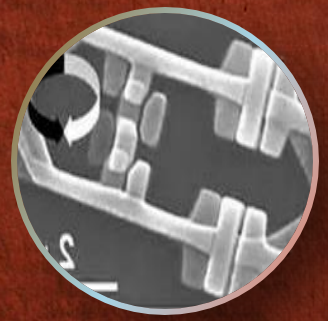
Charlie Marcus' Lab in Copenhagen, Denmark

One of our primary experimental collaborators

BlueHat IL



Ion traps

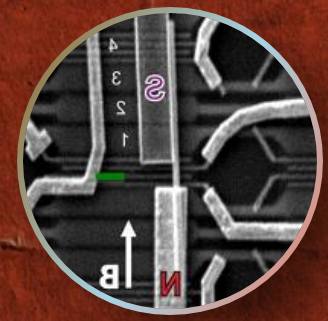


Super-conductors

Linear optics

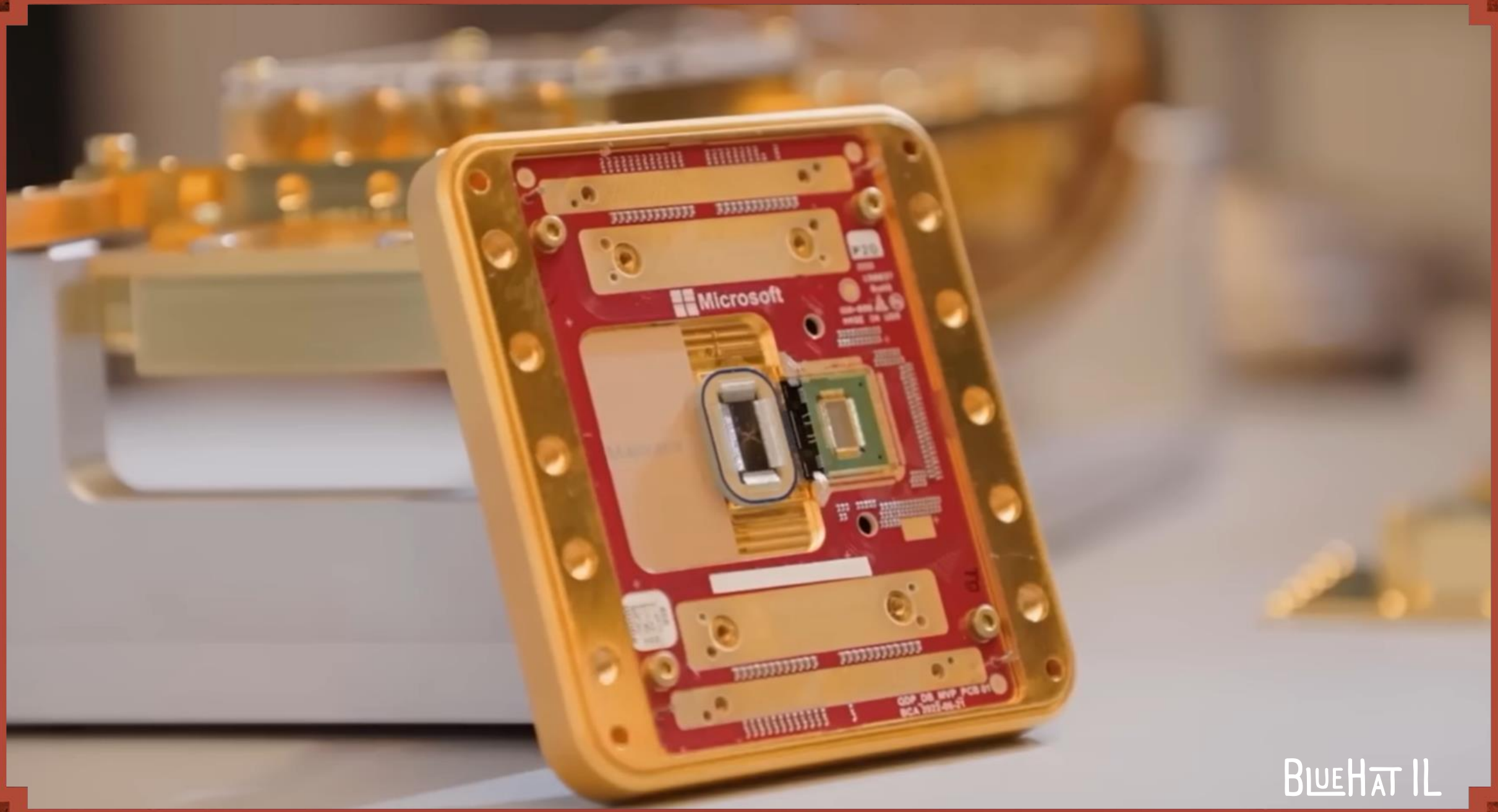
NV centers

Quantum dots



Topological

BlueHat IL


Microsoft
BlueHat IL

The Science Behind Our Qubit

- A quantum computer needs qubits that are small, fast, and reliable
- The most promising type of qubit required a physics breakthrough: a brand-new state of matter, a Topological state

Three states of matter

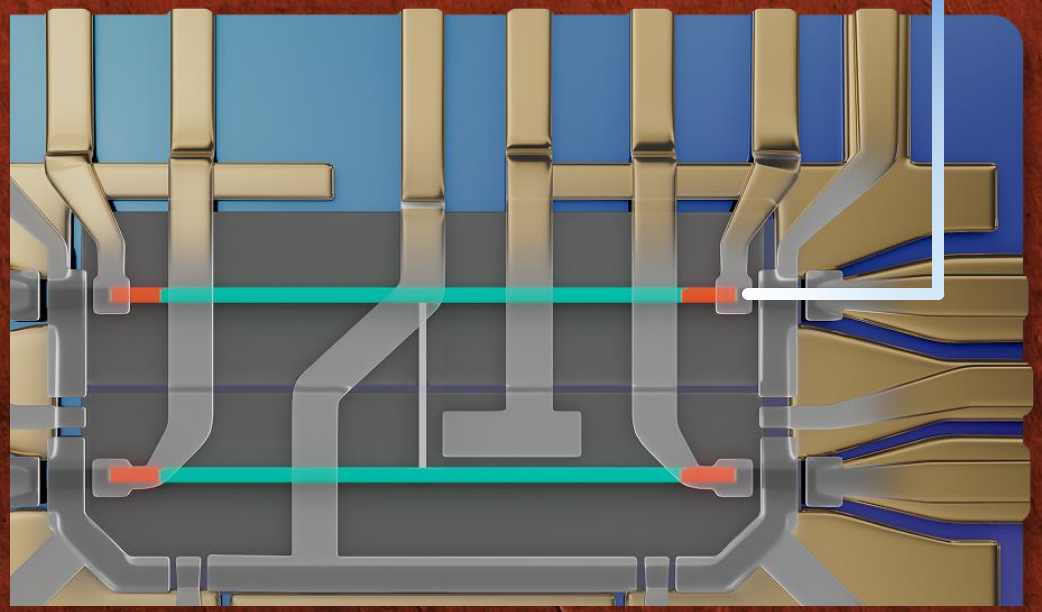
Solid Liquid Gas

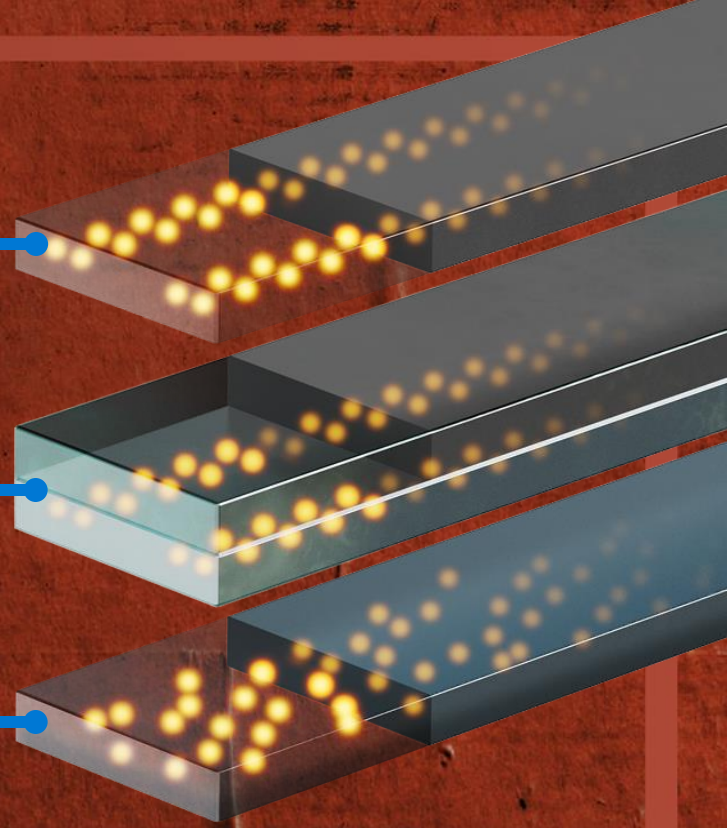
BlueHat IL

• MICROSOFT QUBITS

Topoconductor, a New State of Matter

Materials are key to the creation and control of Majorana.





Superconductor

A material where electricity flows with zero resistance.

Topoconductor

A protected form of matter.

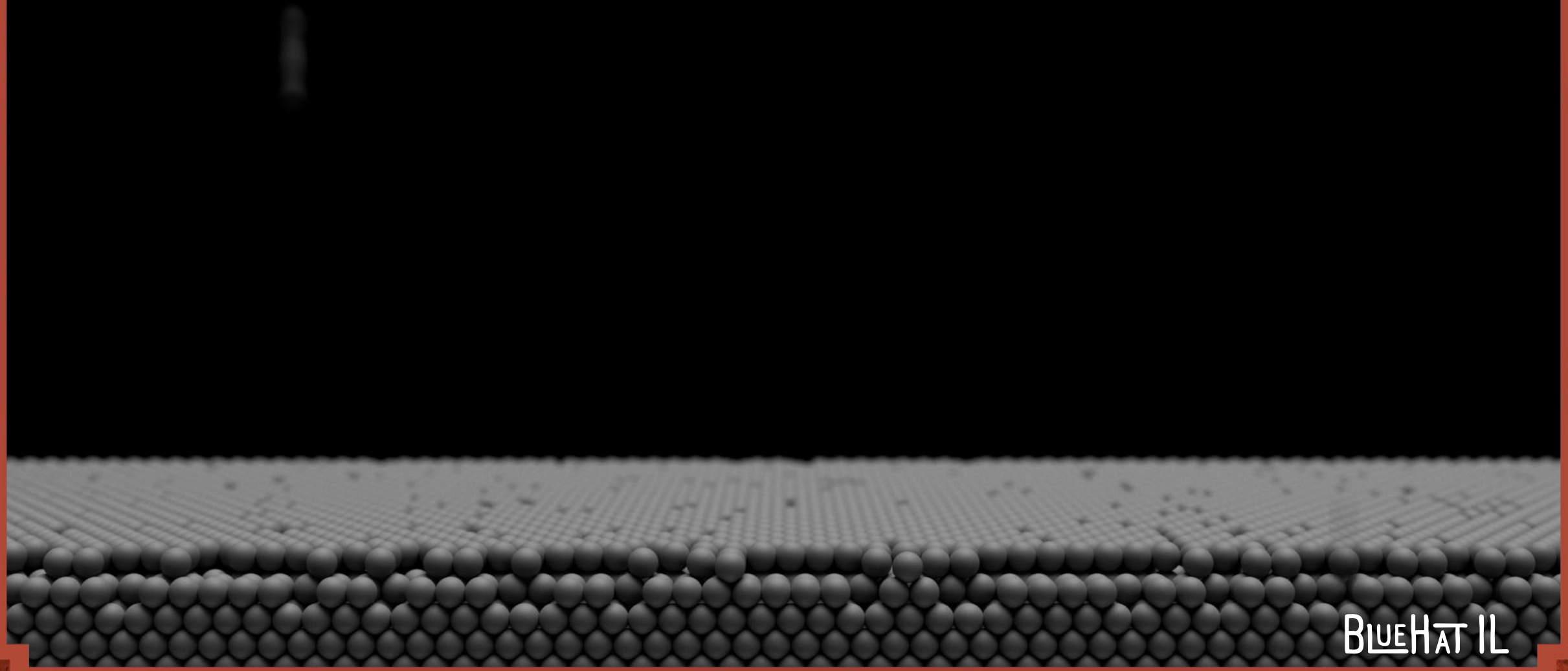
Semiconductor

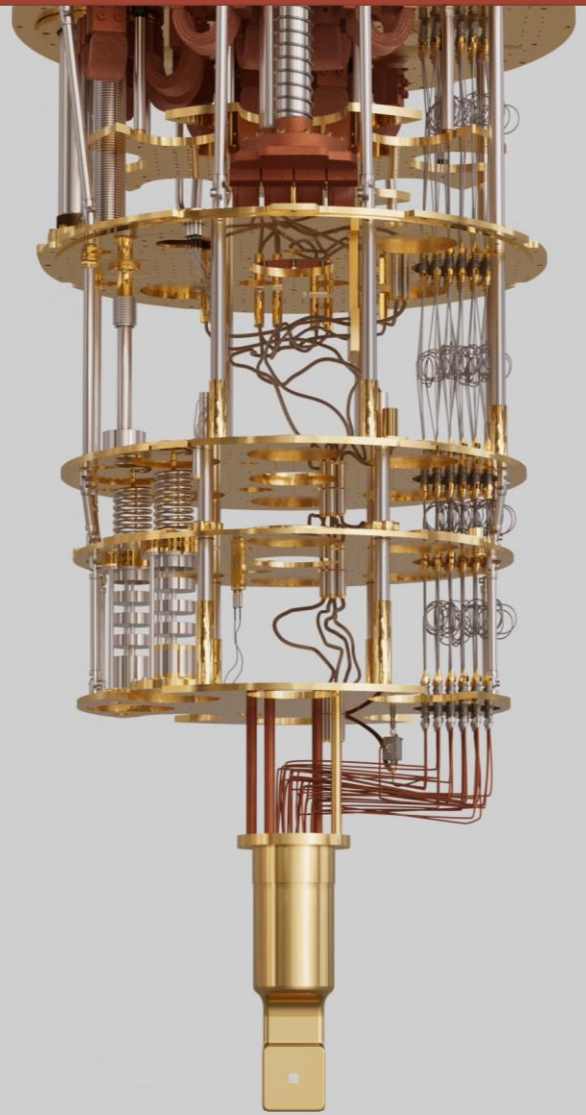
A material that allows precise control of electron density.

The world's first topoconductor

Layers of materials act as one quantum material and exhibit topological properties.

Devices are Built Atom by Atom



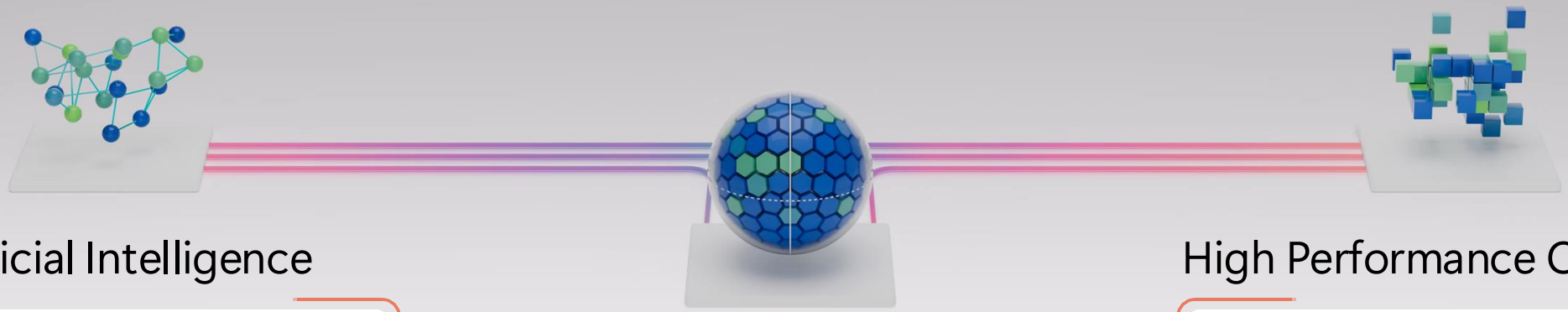


BlueHat IL

Designed to scale
to one million qubits
on a single chip

Fast and digitally
controlled

Microsoft Quantum Compute Platform



Artificial Intelligence

Intelligent reasoning engine in Copilot

Accelerated simulation

High throughput generation and screening

Quantum

Quantum Compute System

Quantum Services

Quantum Processing Units (QPUs)

atom computing · QUANTINUUM · IONQ · PASQAL · photonic · qci · rigetti

High Performance Computer

Optimized chemistry and materials science codes

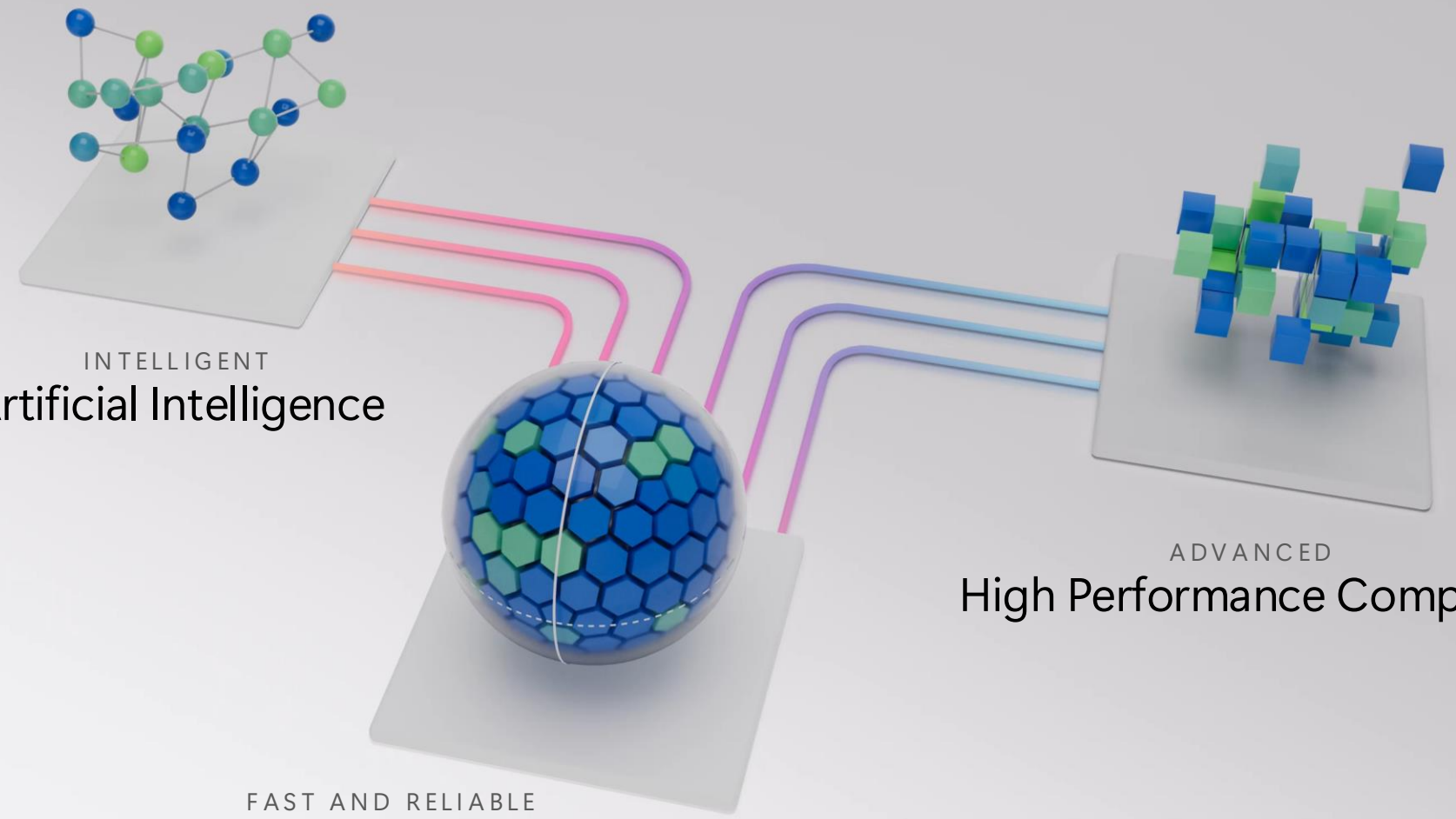
Advanced hybrid workflows

Integration with quantum subroutines

BlueHat IL

Next Generation Applications Require a

Hybrid Compute Platform



INTELLIGENT

Artificial Intelligence

ADVANCED

High Performance Computer

FAST AND RELIABLE

Quantum

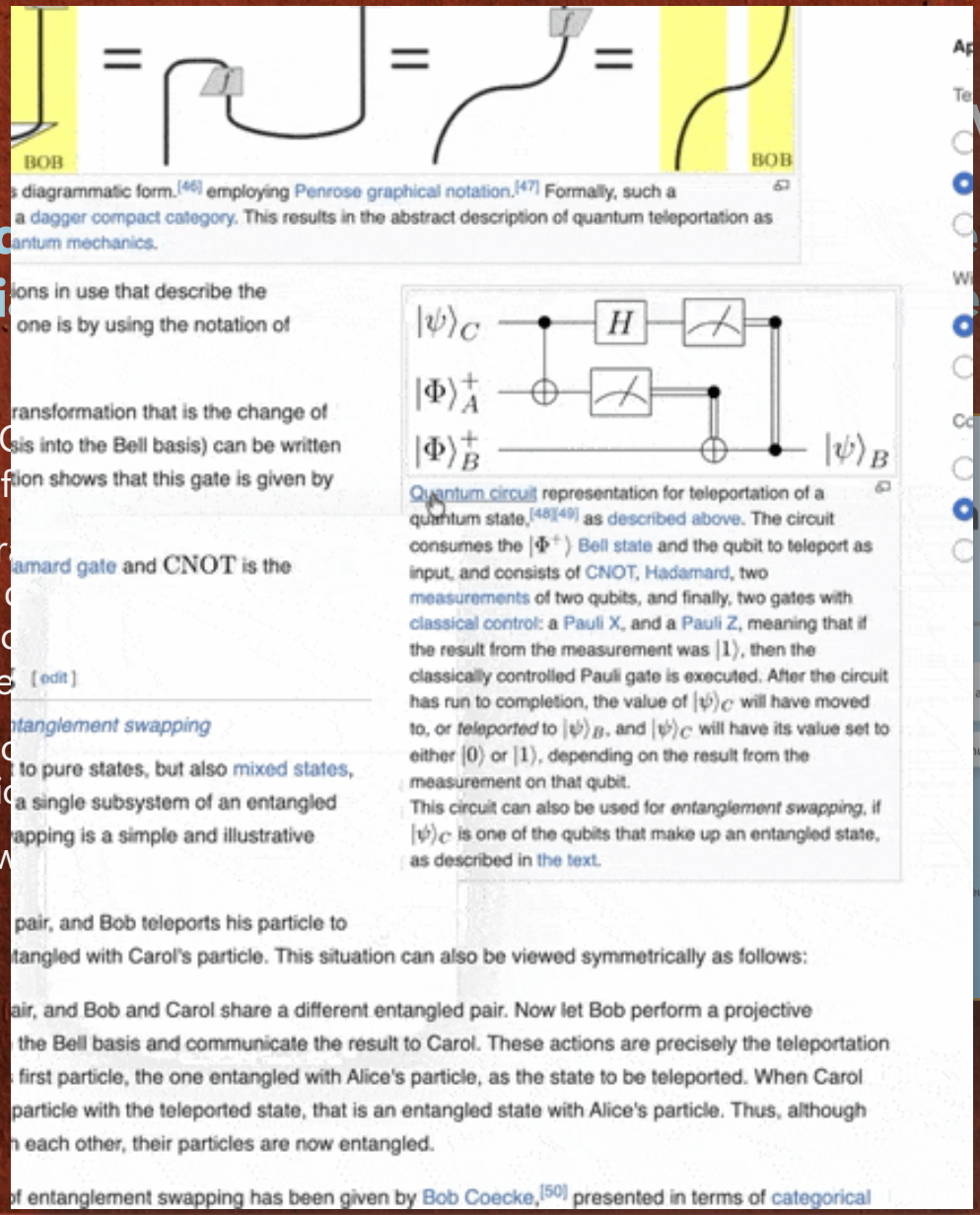
BlueHat IL

Expanding the

End-to-end, AI-enhanced
applications using famili

- Fully integrated with VS Code and C
  Copilot to simplify the use of QDK f
- Includes Python and Jupyter integr
  rendering, IntelliSense, breakpoint
  local simulators, visualizations, histo
  hardware submission, and resource
- Conduct programming tasks like co
  generation, unit tests, job submissi
- Build quantum applications faster w
  AI-assisted development

https://github.com/microsoft/qdk

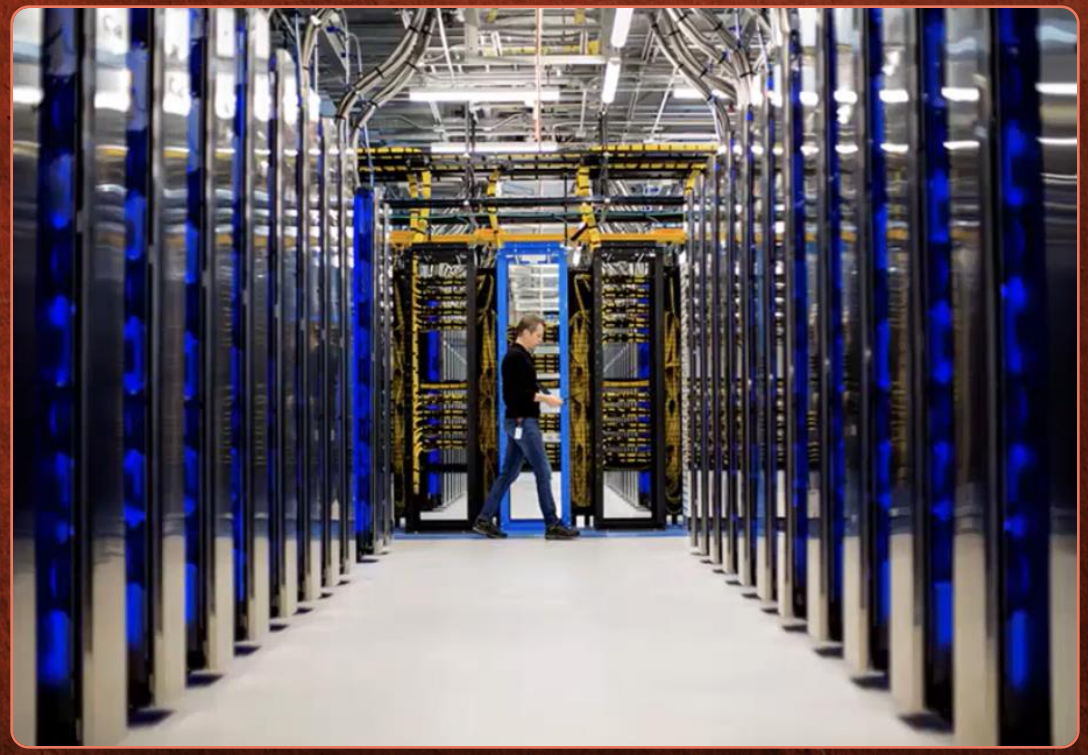


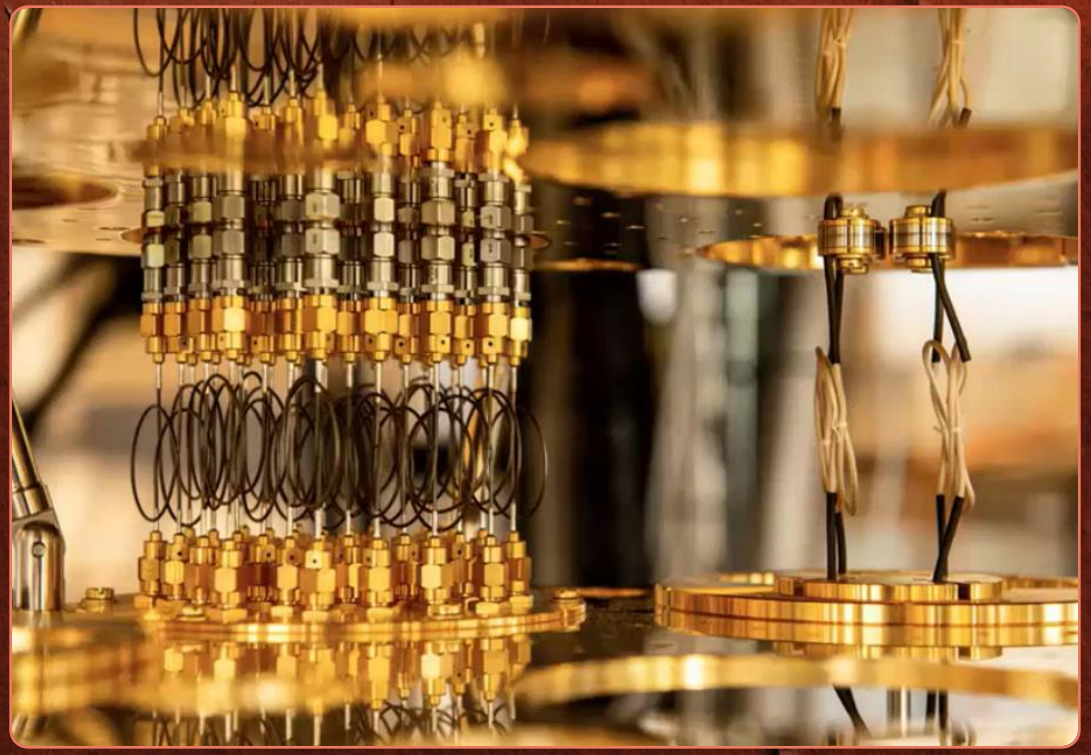
velopment Kit

al quantum
roperable languages

BlueHat IL

Practical Quantum Advantage



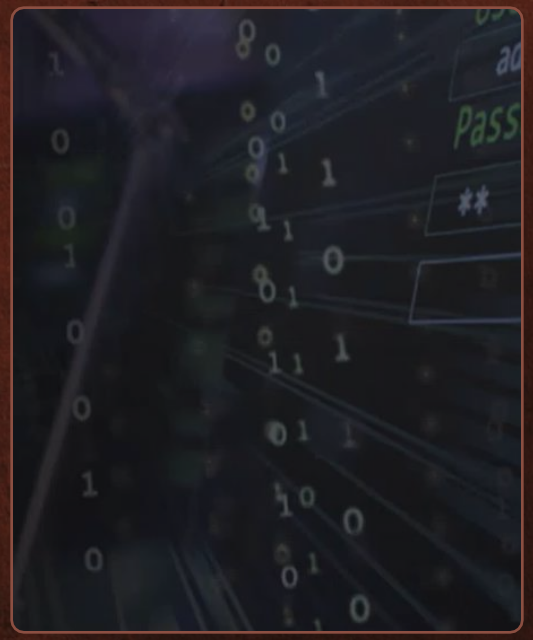


Solve a problem that is useful either for academics or industry faster or better than any known classical algorithm on the best classical computer

BlueHat IL

Areas of Quantum Impact

CRYPTOGRAPHY



Quantum systems SIMU

FINANCIAL TIMES

HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION LEX WORK & CAREERS LIFE & ARTS HTSI

Moral Money Climate change + Add to myFT

What can quantum computers do for humanity?

PsiQuantum chief executive argues technology could yield breakthroughs against climate change and disease

Simon Mundy

Published YESTERDAY

MACHINE LEARNING

BlueHat IL

QUANTUM COMPUTING AND THE END OF ENCRYPTION

by: Maya Posch

57 Comments

June 11, 2020

The Quantum-Safe Journey is a Top Priority for Microsoft

We find ourselves in a unique position related to quantum-safe:

We are creators

Engineering a quantum supercomputer, and developing PQC since 2014

We are systems managers

More than 200k people, 120 geographies, complex scale IT

We are a service provider

hyper-scale cloud computing with Azure and Microsoft 365

We are a security provider

Comprehensive coverage across platforms and cloud for end-to-end protection

Microsoft understands the importance of the complete ecosystem and addressing it holistically

BlueHat IL

Microsoft | Microsoft Security Why Microsoft Security Solutions Products Pricing Services Partners Resources Contact Sales Start free trial All Microsoft Search Light Dark

Home > Quantum-safe security: Progress towards next-generation cryptography

Search the blog

August 20 • 6 min read

Quantum-safe security: Progress towards next-generation cryptography

By Mark Russinovich and Michal Braverman-Blumenstyk

SHARE

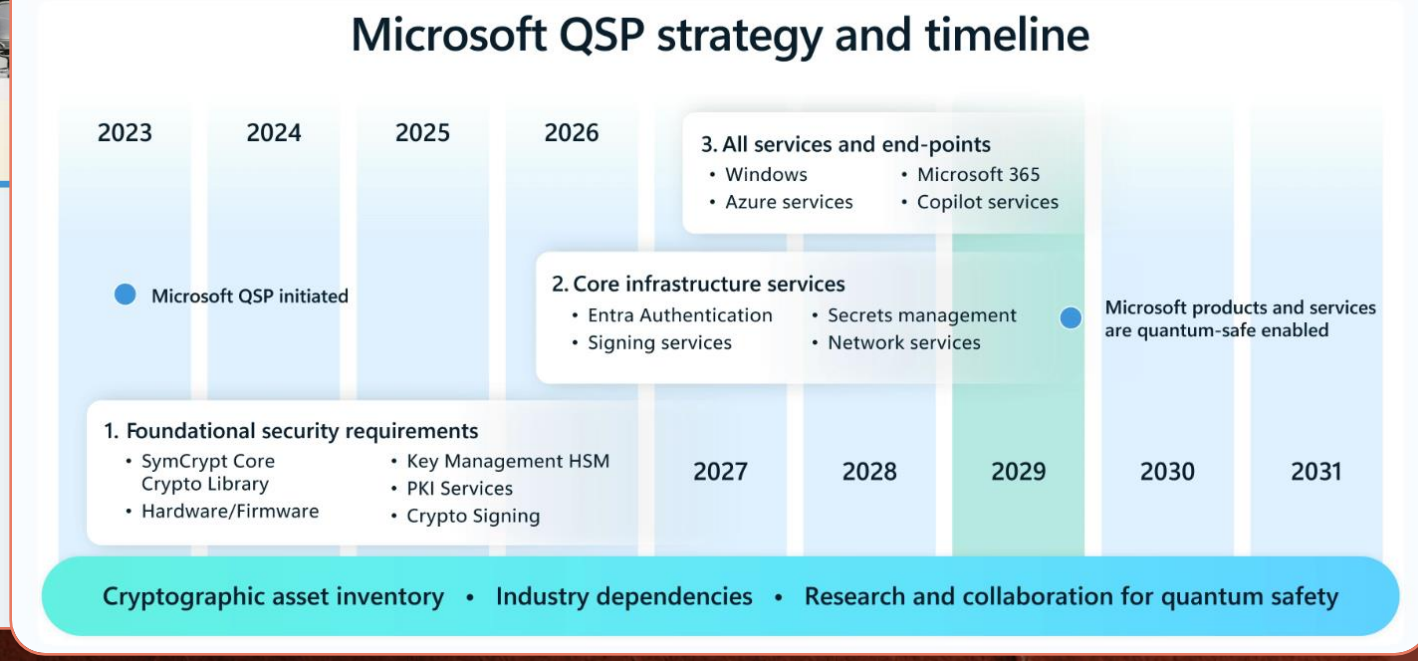
Quantum computing promises transformative advancements, yet it also poses a very real risk to today's cryptographic security. In the future scalable quantum computing could break public-key cryptography methods currently in use and undermine digital signatures, resulting in compromised authentication systems and identity verification.

STARTING YOUR JOURNEY TO BECOME QUANTUM-SAFE

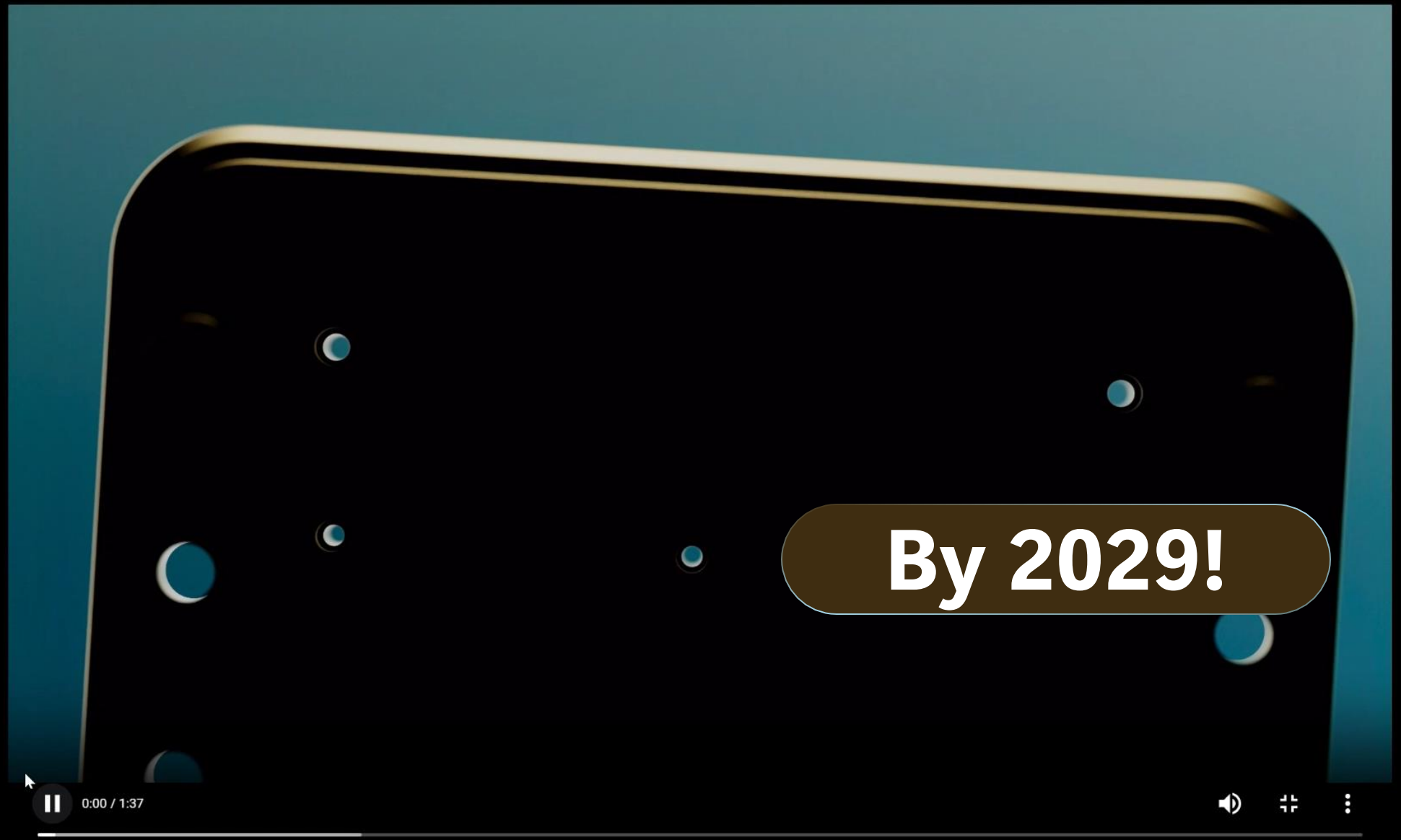
Read the blog ›

While scalable quantum computing is not available today, the time to prepare is now. Microsoft is preparing to be quantum-safe and partnering with regulatory and technical bodies like the National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF), International Organization for Standardization (ISO), Distributed Management Task Force (DMTF), Open Compute Project (OCP), and European Telecommunications Standards Institute (ETSI) to align on quantum-safe encryption standards and support worldwide interoperability.

The opportunity and challenge ahead



BlueHat IL


By 2029!
0:00 / 1:37

Any Sufficiently Advanced Technology is Indistinguishable From Magic.

Arthur C. Clarke

BlueHat IL

BlueHat IL

Dr. Tomer Simon

Partner Chief Scientist, Microsoft Security