The Intersection of Quantum Computing, Artificial Intelligence and Cryptography

—

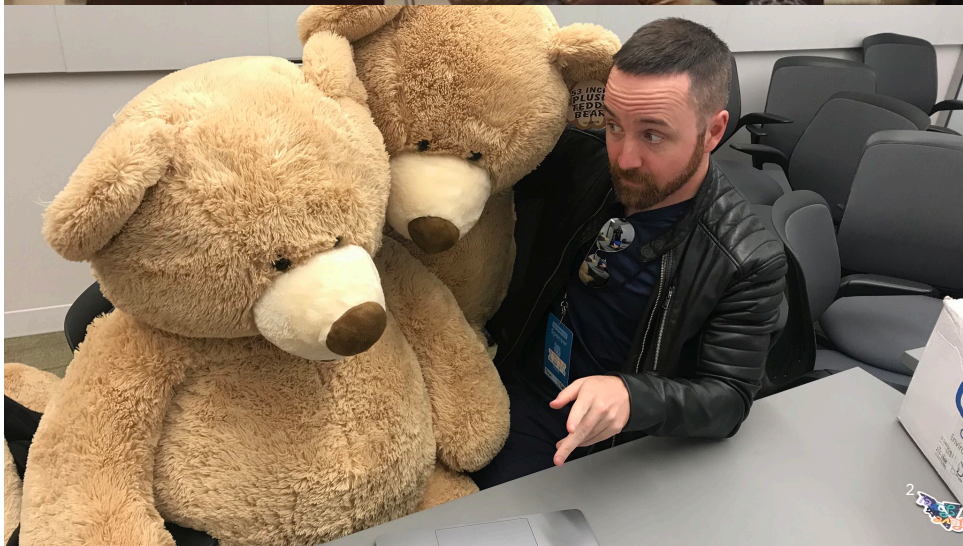
David Nugent
Developer Advocate,
Cognitive, Data & Analytics

Hi, I’m Dave

I’m a developer advocate for IBM in San Francisco. I also help organize:

- The SF JavaScript Meetup
- IBM Developer SF Meetup
- ForwardJS San Francisco && Ottawa

I participate in meetups, hackathons, webinars and write articles about technology for IBM and other organizations.



Agenda

Step 0: Sign Up for IBM Cloud Account

ibm.biz/QuantumWebinar

Defining Artificial Intelligence:

“By AI we mean anything that makes machines act more intelligently. Our work includes basic and applied research in machine learning, deep question answering, search and planning, knowledge representation, and cognitive architectures.”

IBM Research

Americans who say AI has had a mostly or very positive impact on their lives:

79%

Americans who say increased use of AI will eliminate more jobs than it creates:

73%

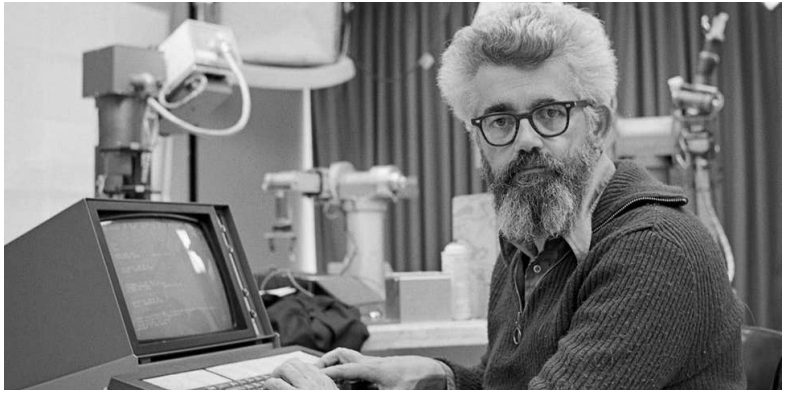
↳ A Brief History of Artificial Intelligence

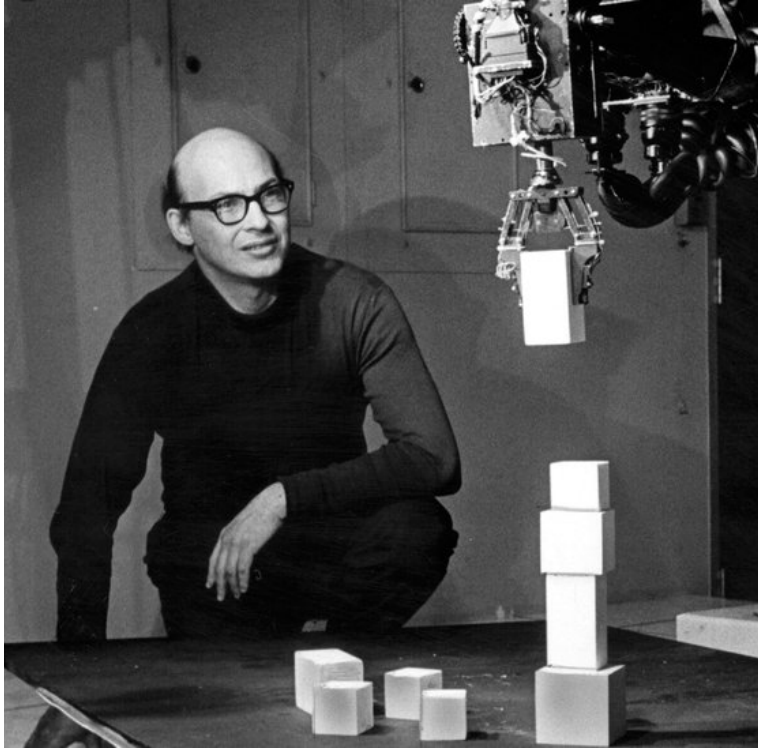
“I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted.”

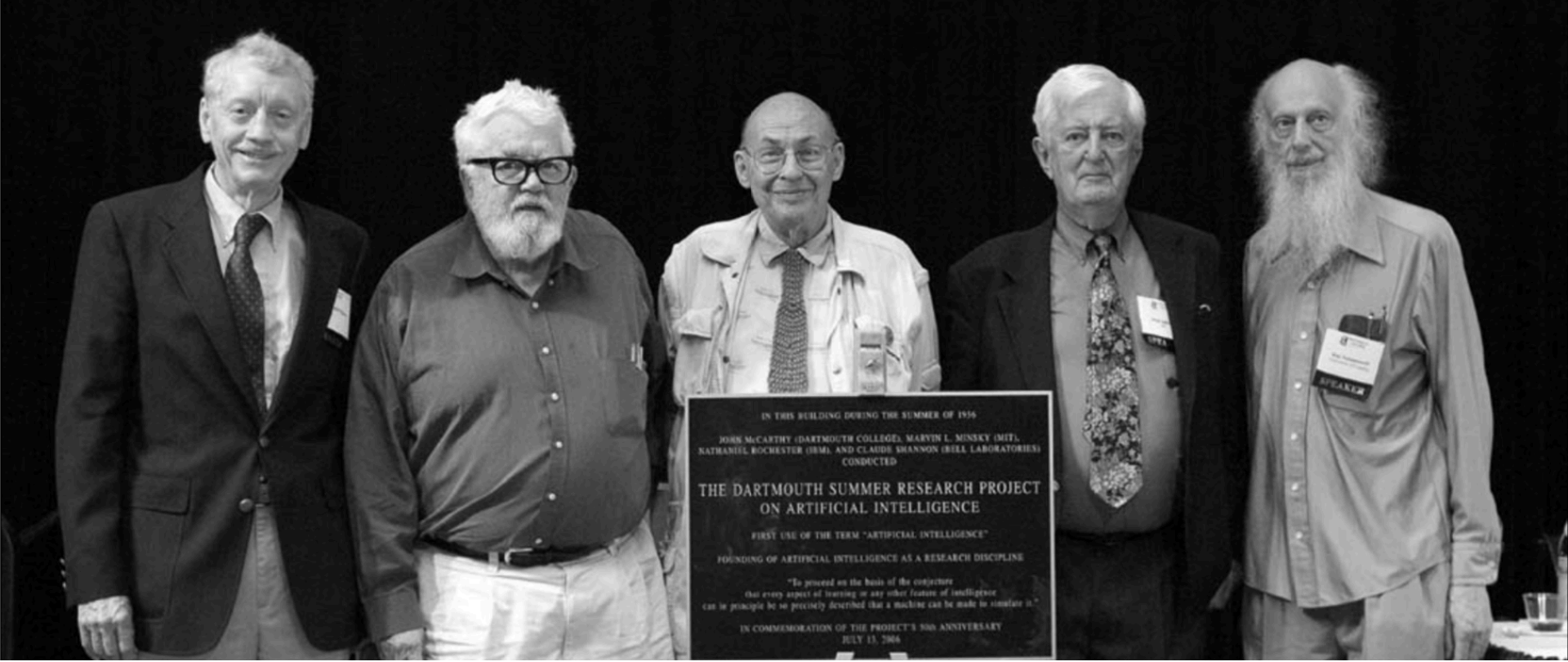
Alan Turing
Computing Machinery and Intelligence

DSRPAI Organizers

John McCarthy and
Marvin Minsky





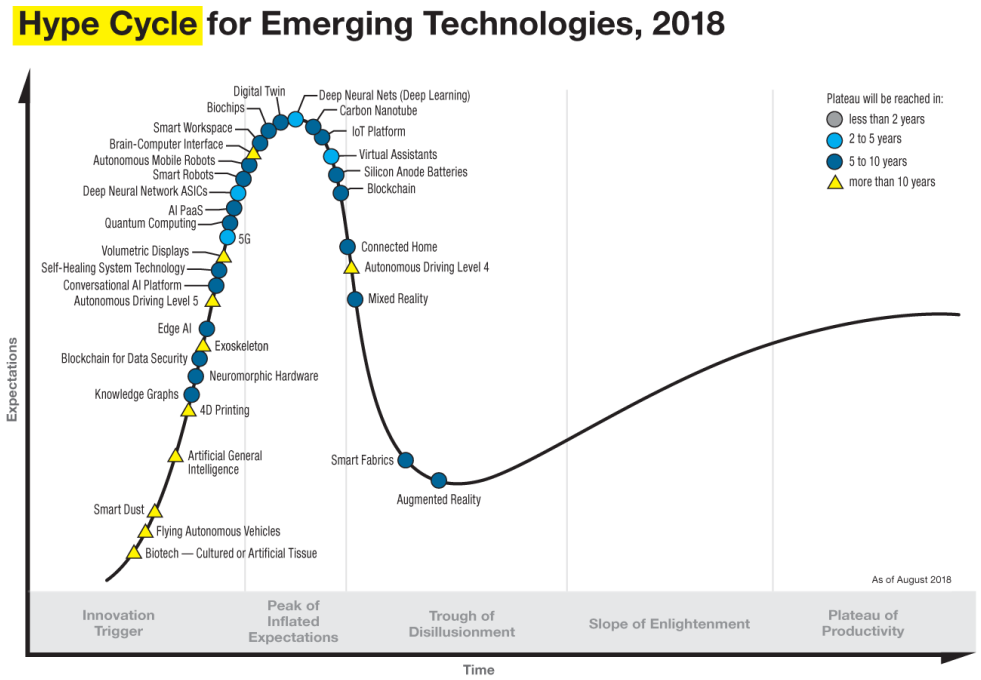


Attendees of Dartmouth Summer Research Project on Artificial Intelligence (DSRPAI) 50 years after the conference: Figure 1. Trenchard More, John McCarthy, Marvin Minsky, Oliver Selfridge, and Ray Solomonoff. Photo by Joe Mehling

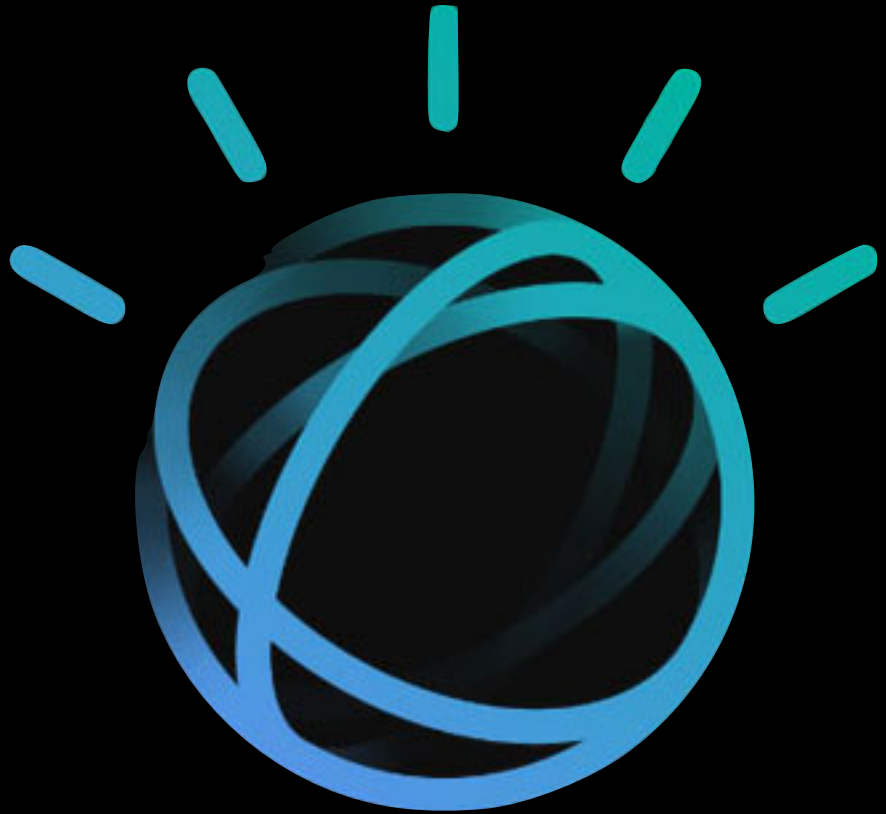
The Gartner Hype Cycle

Artificial intelligence has been an emerging technology for decades, with amazing promises and occasional troughs of disillusionment. These are called “AI winters”

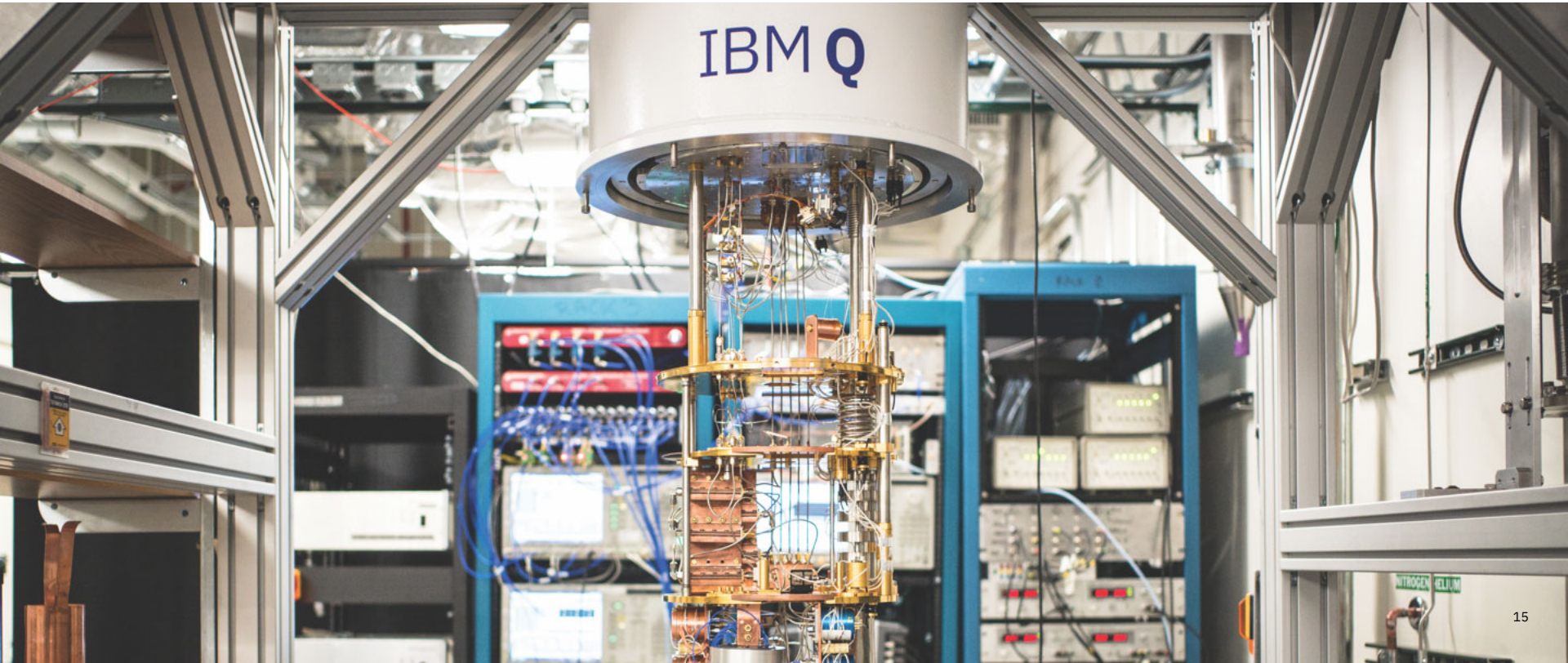
Many current emerging technologies as of 2018/2019 have their roots in AI research



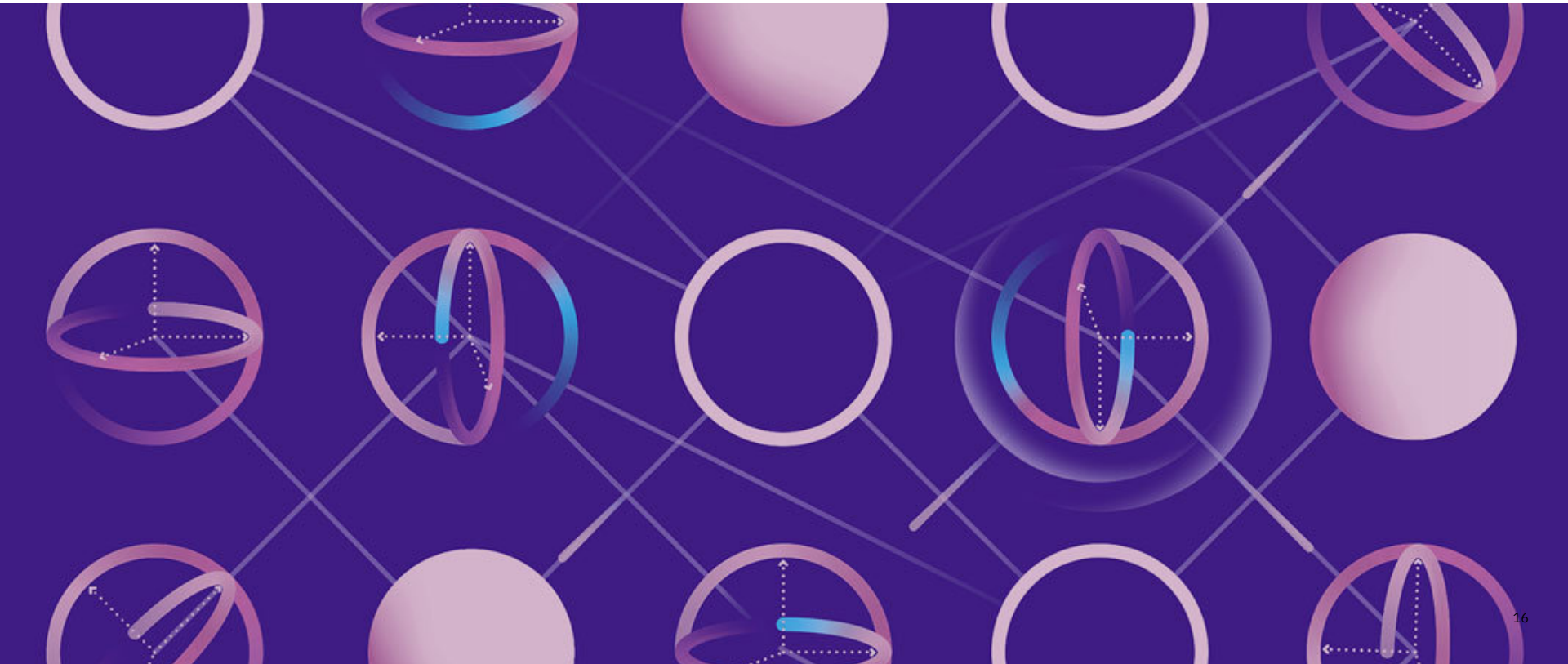
Garry Kaspararov and Deep Blue, 1997



↳ Introduction to Quantum Computing



Quantum Theory



The History of Quantum Theory

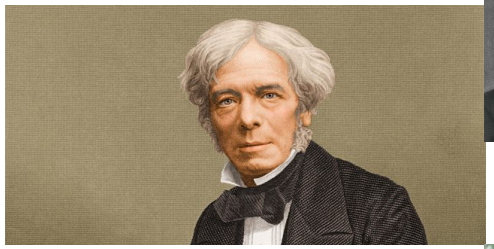
Michael Faraday

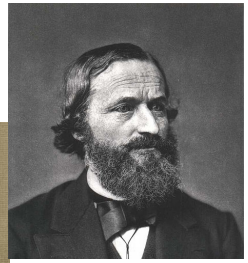
Gustav Kirchoff

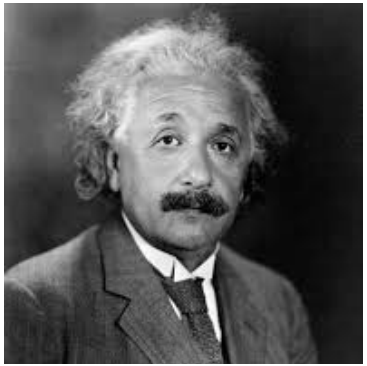
Max Planck

Albert Einstein

Louis de Broglie







Quantum Processors: Superposition

- Classical computers: zeroes and ones
- Quantum computers: zero AND one
- Relationship between qubits and states

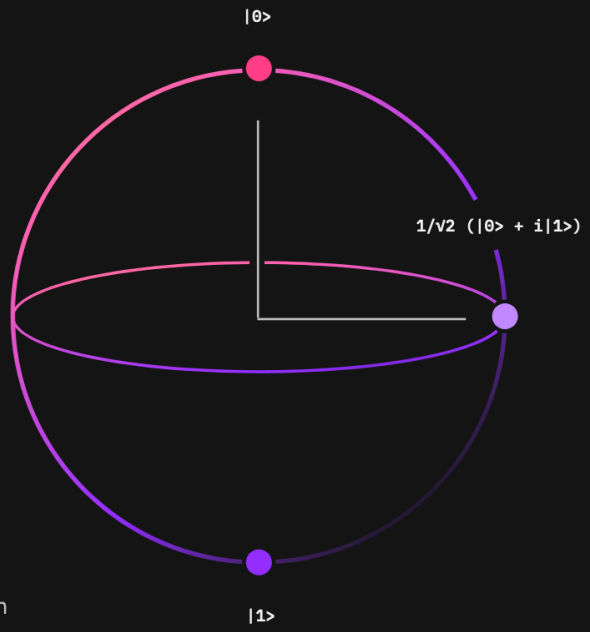


Figure 1:
Superposition

Quantum Processors: Entanglement

Entanglement is a famously counter-intuitive quantum phenomenon describing behavior we never see in the classical world. Entangled particles behave together as a system in ways that cannot be explained using classical logic.

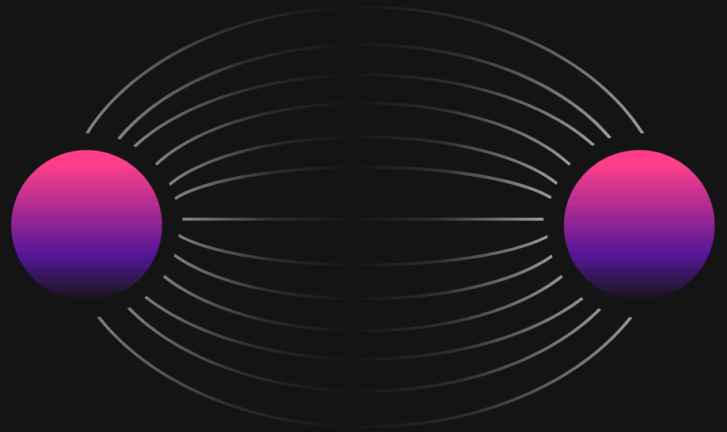


Figure 2: Entanglement

Quantum Processors: Interference

Quantum interference can be understood similarly to wave interference; when two waves are in phase, their amplitudes add, and when they are out of phase, their amplitudes cancel.

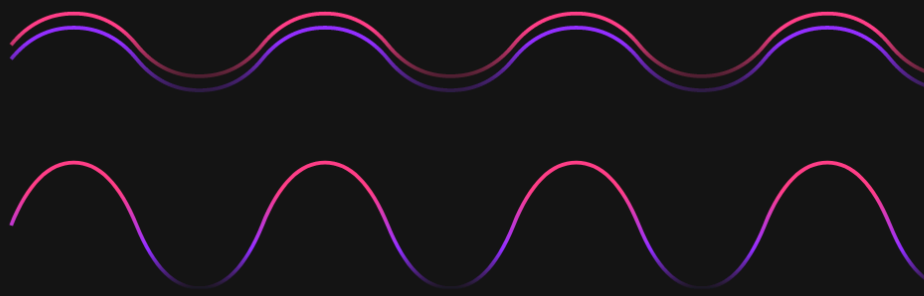
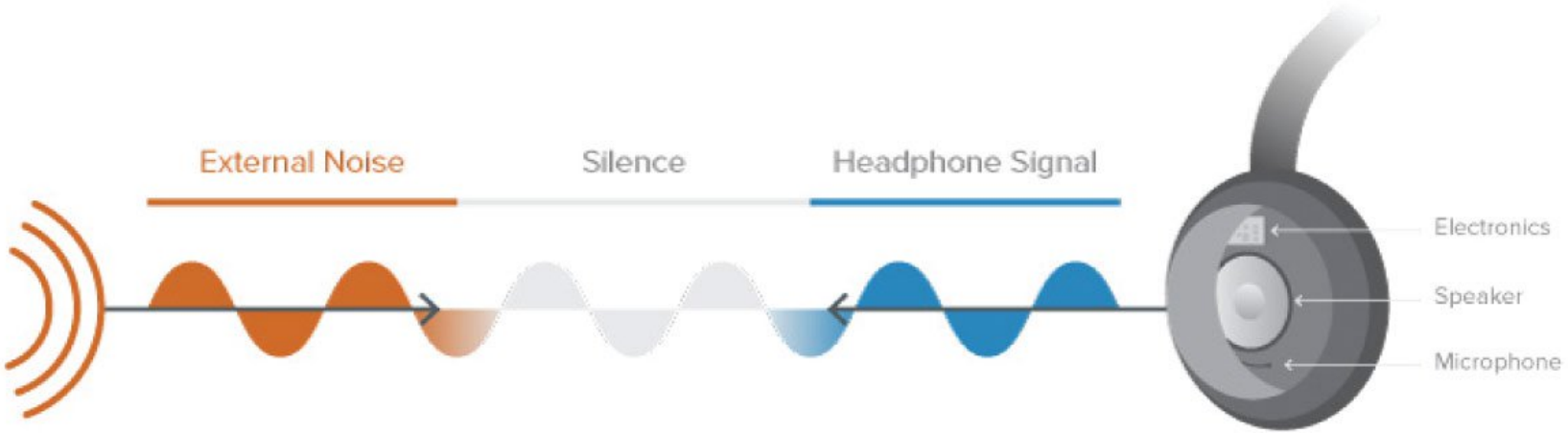


Figure 3:
Positive Interference

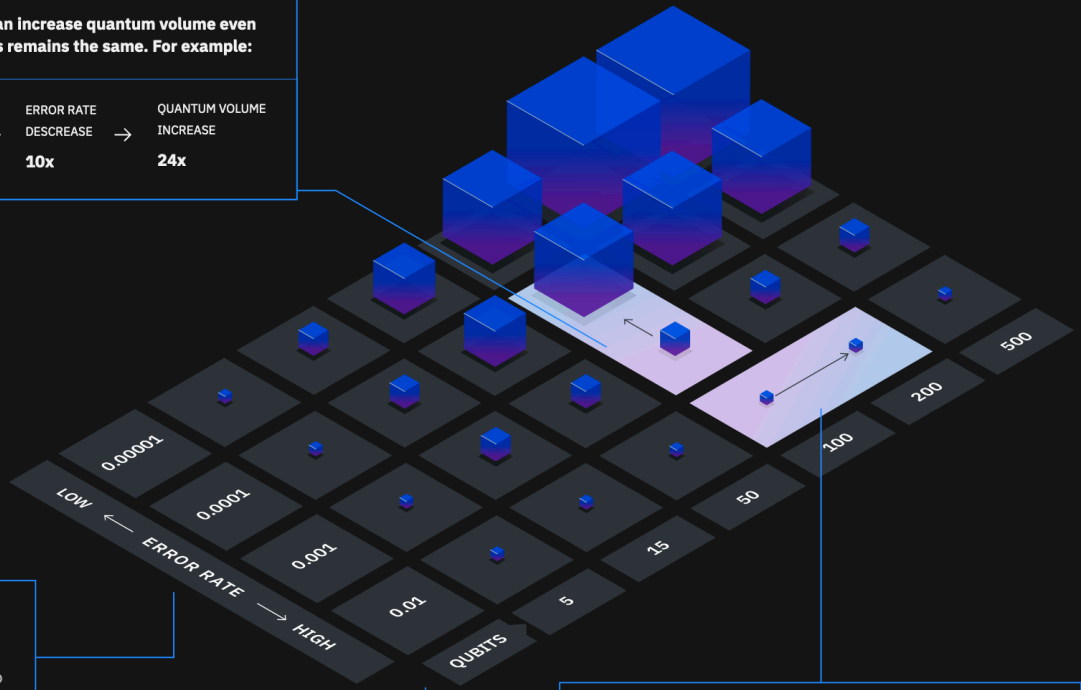
Noise Cancelling Headphones



Scaling Quantum Systems

Improving the error rate can increase quantum volume even when the number of qubits remains the same. For example:

QUBITS EXISTING	→	QUBITS ADDED	→	ERROR RATE DESCREASE	→	QUANTUM VOLUME INCREASE
100 Q		**0 Q**		**10x**		**24x**



Error Rate (Y-Axis)
An expression of how well the device can implement operations between any two qubits

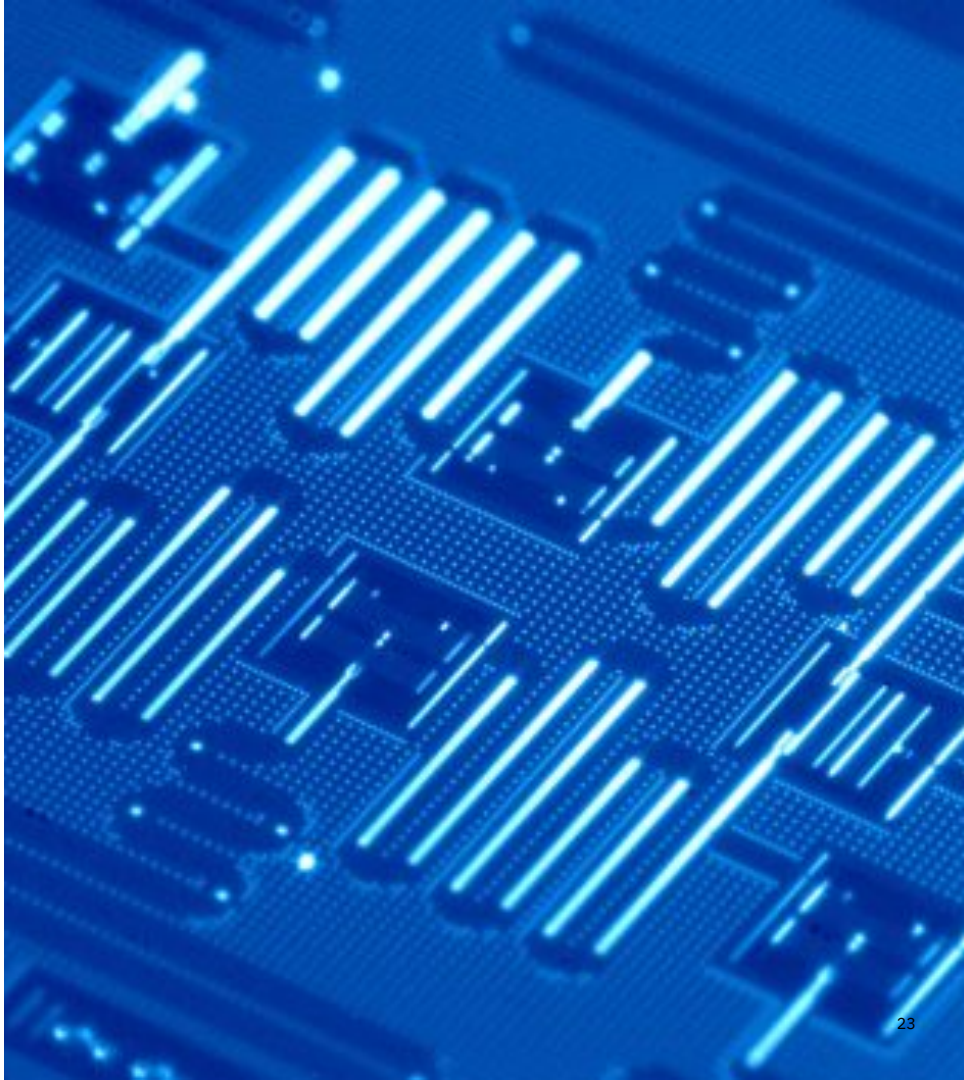
Qubits (X-Axis)
The number of qubits active in the system

If the error rate is high, merely adding qubits will not increase quantum volume.

QUBITS EXISTING	→	QUBITS ADDED	→	ERROR RATE DESCREASE	→	QUANTUM VOLUME INCREASE
100 Q		**100 Q**		**0x**		**0x**

Quantum Computers Inside Out

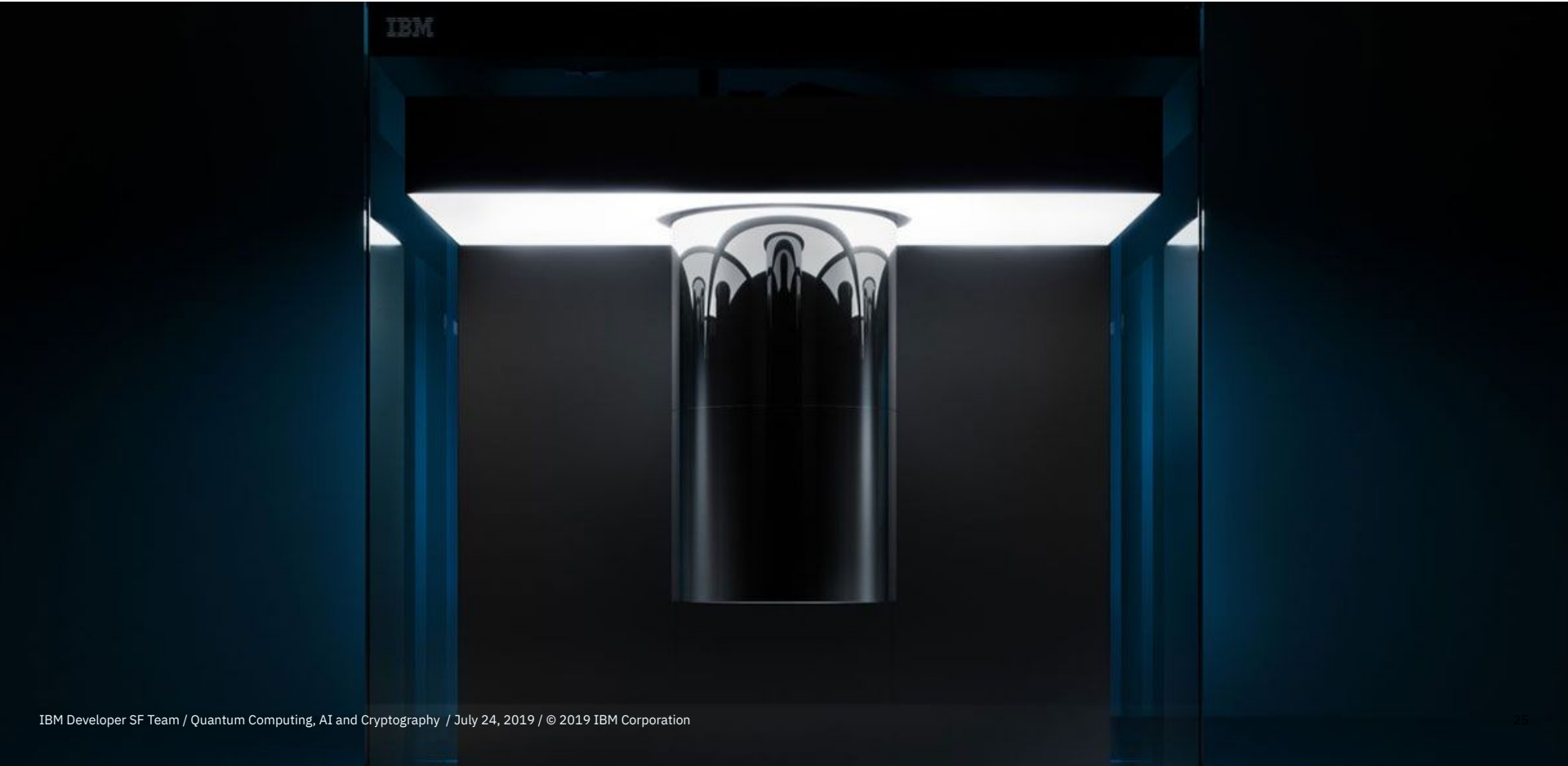
- Superconducting Josephson Junctions
- Macroscopic Quantum Phenomena
- Microwave resonators to address and couple qbits
- Very low temperature



Quantum Computers: Inside Out

IBM Q system inside a dilution refrigerator

Quantum Computers: Inside Out



↳ Quantum Computing, Artificial Intelligence & Cryptography

AI and Crypto Influcence Quantum and Vice Versa

AI controls quantum computers

Auantum states are extremely sensitive to constant interference from their environment. The plan is to combat this using active protection based on quantum error correction. A team has presented a quantum error correction system that is capable of learning thanks to AI.

Quantum computers breaking cryptography

Data that is being stored today using existing cryptography methods will eventually be cracked by quantum computers capable of exponentially faster computational performance. A leading candidate for quantum-safe cryptography standard lies in lattice cryptography.

AI neural networks

A team at Heriot-Watt University hope to produce a breakthrough quantum computer which leads to AI that operates at unprecedented speed, automatically making very complex decisions in a very short time

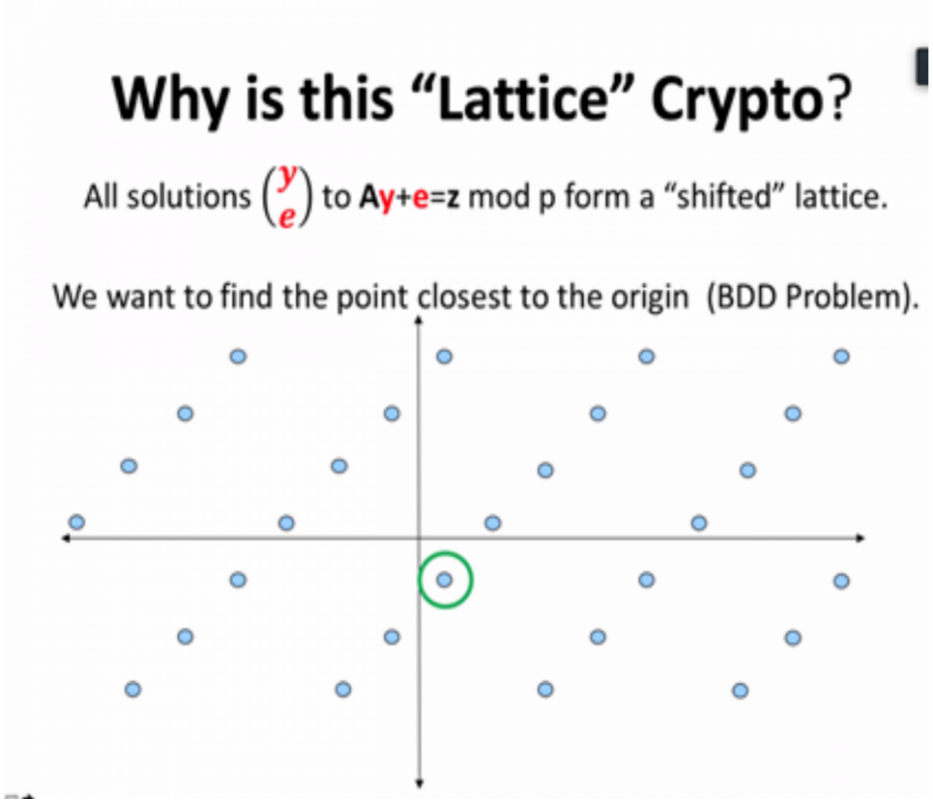
Supervised learning with quantum enhanced feature spaces

As quantum computers become more powerful, they will be able to perform feature mapping on highly complex data structures that classical computers cannot. (IBM is giving away these feature-mapping algorithms via Qiskit Aqua)

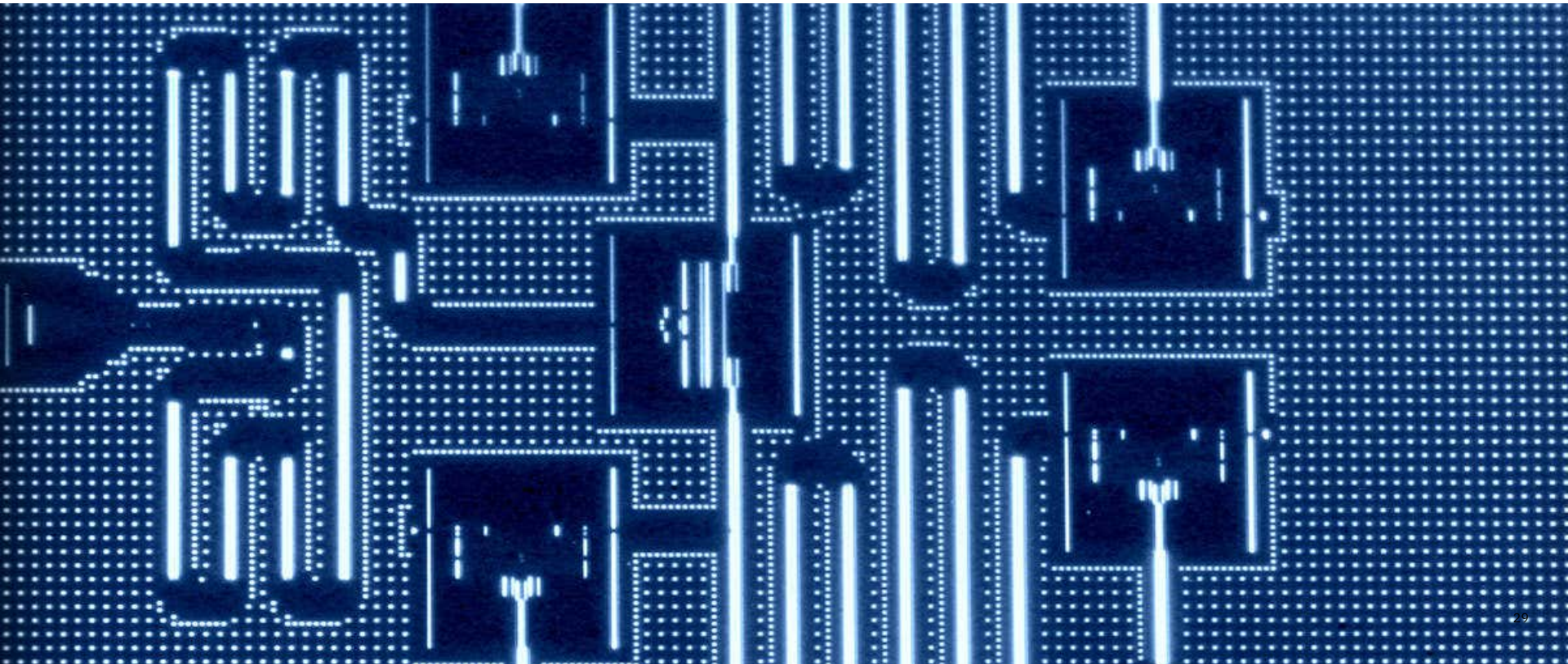
Lattice Field Cryptography

"[L]attice problems have a unique characteristic that will make it reasonably impenetrable by quantum computing. It requires solving for two unknowns – a multiplier array and an offset. [...] it is extremely difficult for quantum computing to solve the lattice problems - the shortest vector problem (SVP) and the closest vector problem (CVP) – upon which lattice cryptography is built."

Forbes



↳ Let’s Code a Quantum Computer



Step 0: Sign Up for IBM Cloud Account

ibm.biz/QuantumWebinar

Step 1: Visit the Q Experience

https://quantum-computing.ibm.com/login

Quantum Computing Demo

“It seems probable that once the machine thinking method had started, it would not take long to outstrip our feeble powers… They would be able to converse with each other to sharpen their wits. At some stage therefore, we should have to expect the machines to take control.”

Alan Turing
Intelligent Machinery, A Heretical Theory
1951

07.26.19

SERVERLESS DEVELOPER SUMMIT

GALVANIZE, SAN FRANCISCO

Part of **IBM Developer – 34 groups**

IBM Developer SF Bay Area

San Francisco, CA

7,619 members · Public group

Organized by **Angie K** and **6 others**

IBM Developer

IBM

WED, JUL 31, 9:30 AM

Online Meetup: Getting started with IBM Blockchain Platform 2.0 in the...

To be determined

RSVP on Crowdcast NOW! https://www.crowdcast.io/e/0w6ccq4v ! Please do not forget to register on Crowdcast and join us using Chrome browser via Crowdcast on the event date! Hyperledger Fabric, the Blockchain framework supported by IB...

38 attendees

Attend

THU, AUG 1, 12:00 PM

Lunch and Learn: IBM Blockchain Platform 2.0 Internals Workshop

44 Tehama St

Join IBM Developer SF's workshop and learn how to develop Blockchain applications with VS Code and deploy them on the IBM Blockchain Platform. The brand new cloud-based IBM® Blockchain Platform provides a managed and full-...

36 attendees

Attend

IBM Partners

Enabling Independent Software Vendors (ISVs) and tech companies for growth

Target audience

- ISVs and tech companies building and selling cloud solutions
- New to IBM Cloud
- Startups who aspire to build and sell their own solutions

Offers to help you get started

Build with up to $12,000 of free IBM Cloud™ credits ($1,000 per month for 12 months)

Integrate your solutions with leading-edge IBM Cloud technologies to deliver more innovation and value to your clients. Access more than **130 unparalleled services** including Watson™, Analytics and Security.

Build with 10TB of IBM Cloud Object Storage at no charge

Build data capability into your offering. IBM Cloud Object Storage is designed for high durability, resiliency and security.

Build with IBM Watson Assistant with a 1-year free trial

Receive access to 100K API calls per month plus 10 workspaces. Build and deploy chatbots quickly and efficiently with IBM Watson Assistant's advanced capabilities and seamless interface.

Build with IBM Cloud Kubernetes Service with a 1-year free trial

Containerize your solution with 1TB of block storage. Ship all your applications in one agile, well-defined structure with IBM Cloud Kubernetes Service.

Build with IBM Blockchain with a 6-month free trial

Build a network with up to 3 organizations to prototype. Build a secure business transaction network for your clients using blockchain and smart contracts.

Finished building and testing? Go-to-market with IBM

Access Provider Workbench, attend an orientation session and join the premier network of over 400 partners who are already listing their solutions on the IBM Marketplace.

Is your business a Startup? Build with up to $120,000 in IBM Cloud credits

If your business revenue in the last 12 months is less than $1M and you've been in business for fewer than five years, then you may qualify for Startup with IBM.

Get started

Experience IBM's countless partner benefits. Start building and selling with IBM today.

Learn more and access offers at ibm.com/partners/start