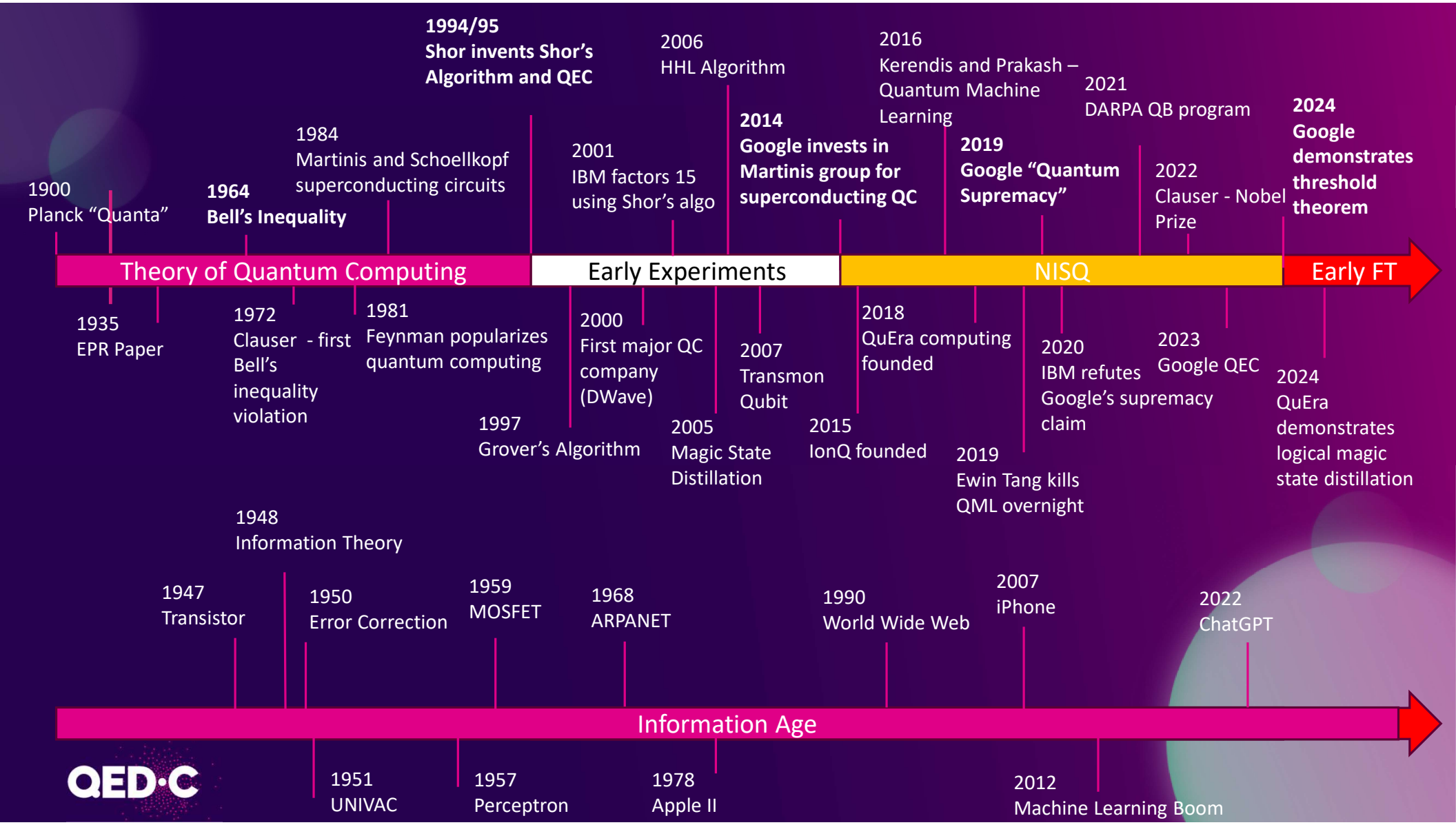
Quantum 101

Bruno Avritzer, Ph.D.

Vice-Chair, QED-C Standards and Performance Benchmarks TAC

30 June 2026

**Disclaimer: Any opinions expressed here are my own and do not necessarily reflect the positions of Leidos or the QED-C


1994/95
Shor invents Shor's Algorithm and QEC
2006
HHL Algorithm
2016
Kerendis and Prakash – Quantum Machine Learning
2021
DARPA QB program
2024
Google demonstrates threshold theorem
1900
Planck "Quanta"
1964
Bell's Inequality
1984
Martinis and Schoellkopf superconducting circuits
2001
IBM factors 15 using Shor's algo
2014
Google invests in Martinis group for superconducting QC
2019
Google "Quantum Supremacy"
2022
Clauser - Nobel Prize
Theory of Quantum Computing
Early Experiments
NISQ
Early FT
1935
EPR Paper
1972
Clauser - first Bell's inequality violation
1981
Feynman popularizes quantum computing
2000
First major QC company (DWave)
2007
Transmon Qubit
2018
QuEra computing founded
2020
IBM refutes Google's supremacy claim
2023
Google QEC
2024
QuEra demonstrates logical magic state distillation
1997
Grover's Algorithm
2005
Magic State Distillation
2015
IonQ founded
2019
Ewin Tang kills QML overnight
1948
Information Theory
1947
Transistor
1950
Error Correction
1959
MOSFET
1968
ARPANET
1990
World Wide Web
2007
iPhone
2022
ChatGPT
Information Age
1951
UNIVAC
1957
Perceptron
1978
Apple II
2012
Machine Learning Boom

Quantum Analogs of Classical Things

Classical Concept	Quantum Concept	Key Difference
Bit	Qubit (Quantum Bit)	Bits are integers, qubits are vectors
Information Theory	Quantum Information Theory	Uses rules of quantum probability
Computer	Quantum Computer	Probabilistic computation with quantum probability rules
Communication Network	Quantum Network	Can exploit correlations for FTL coordination (NOT communication)
Forward Error Correction	Quantum Error Correction	Compute on encoded information without decoding
Transistor	Quantum Transistor (Logical Qubit)	Requires quantum error correction
Fiber Repeater	Quantum Repeater	Fundamental loss limit of 3dB (50%)
Sensor	Quantum Sensor	Uses entanglement to beat classical sensitivity limits

Quantum Information Theory

The Quantum Information Revolution

0

1

0+1

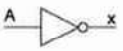
00+11

If you flip a coin, at the end of the day it lands on heads or tails.

QED·C

Quantum Logic

Classical

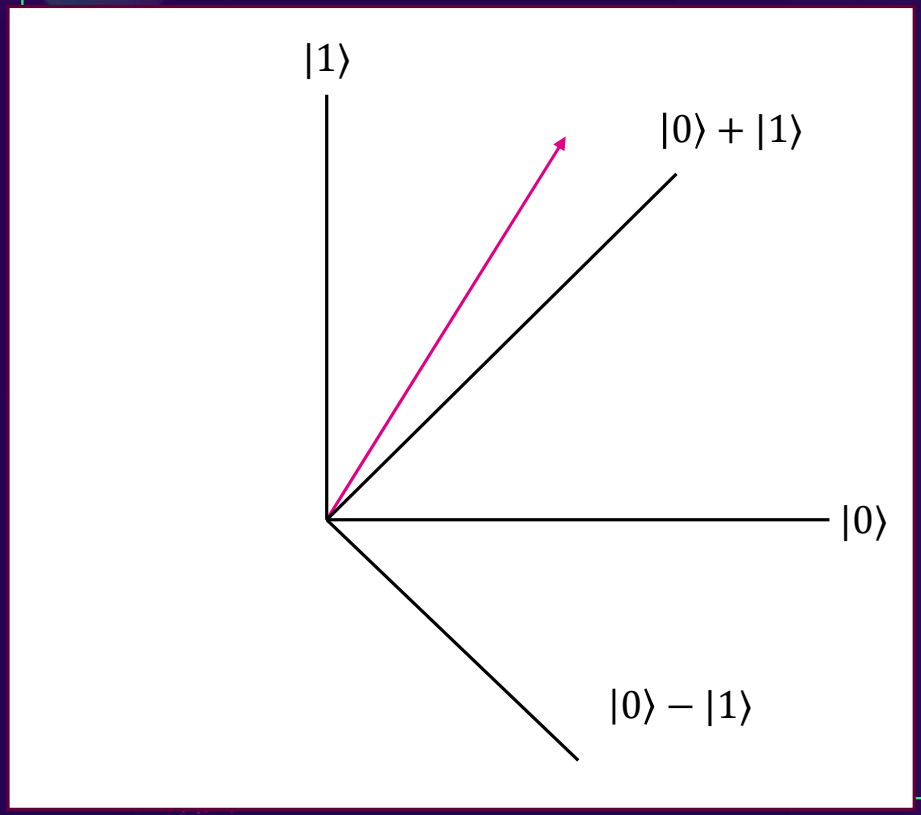
Name	NOT	AND	NAND	OR	NOR	XOR	XNOR
Alg. Expr.	$\overline{A}$	AB	$\overline{AB}$	$A+B$	$\overline{A+B}$	$A \oplus B$	$\overline{A \oplus B}$
Symbol							
Truth Table	A X 0 1 1 0	B A X 0 0 0 0 1 0 1 0 0 1 1 1	B A X 0 0 1 0 1 1 1 0 1 1 1 0	B A X 0 0 0 0 1 1 1 0 1 1 1 1	B A X 0 0 1 0 1 0 1 0 0 1 1 0	B A X 0 0 0 0 1 1 1 0 1 1 1 0	B A X 0 0 1 0 1 0 1 0 0 1 1 1

Quantum

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

QED·C

Quantum Logic



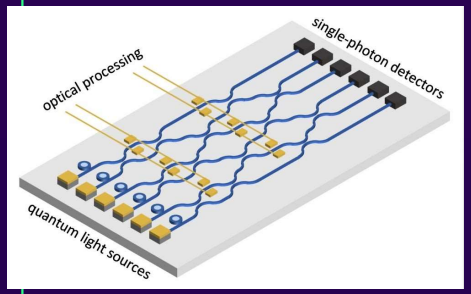
0+1

0-1

QED·C

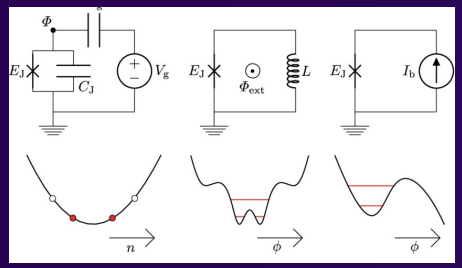
Types of Quantum Processors

Photonic



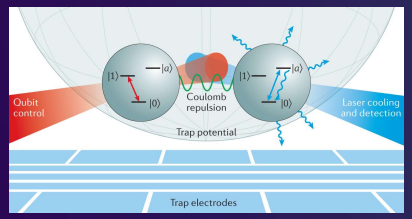
- Medium speed
- Ok lifetime
- Terrible CNOT efficiency
- Scales well on paper

Superconducting



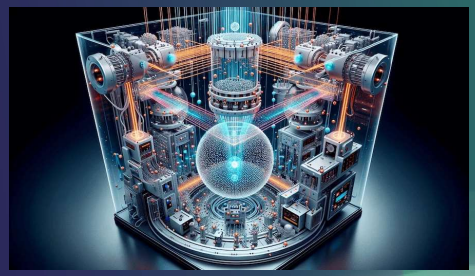
- Fastest
- Poor lifetime
- Most mature today
- Poor scaling

Trapped Ion



- Slow
- Best lifetime
- Scale with networking

Neutral Atom

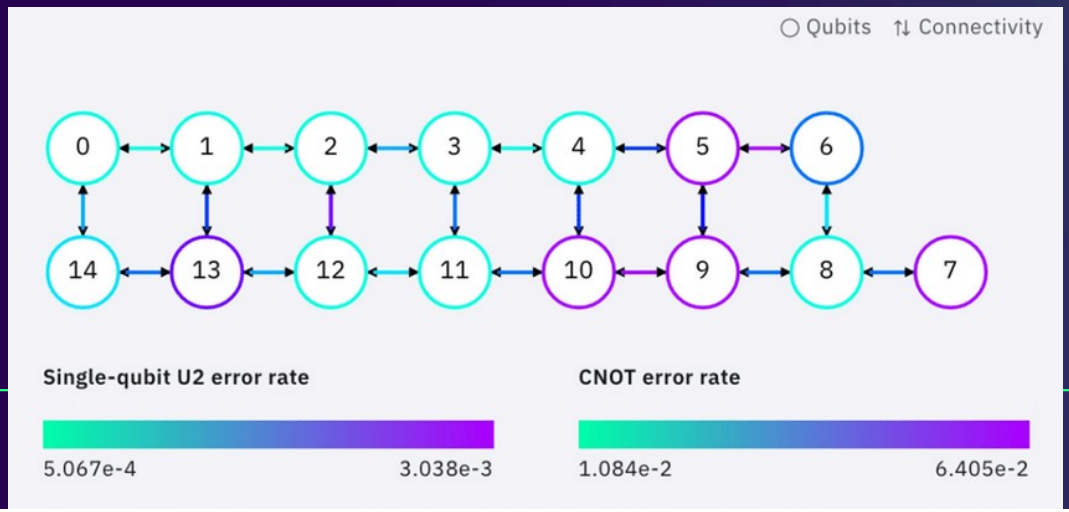


- Medium speed
- Good lifetime
- Scales very well up to tens of thousands of qubits

QED·C

The NISQ Era

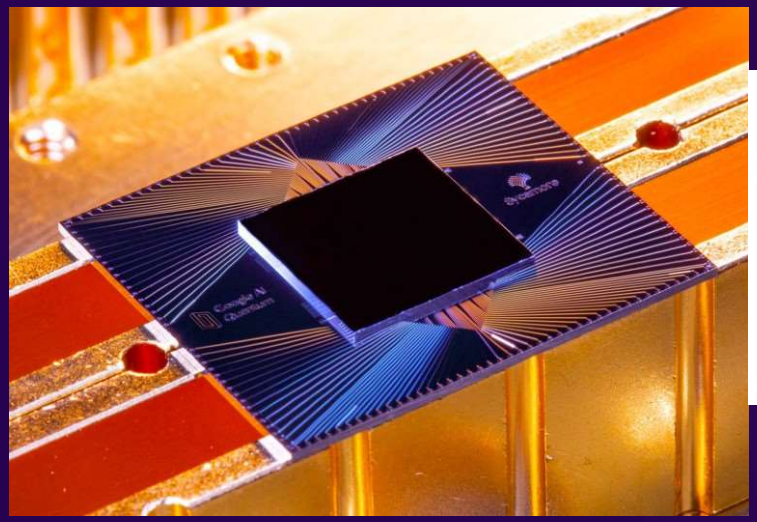
- **NISQ - N**oisy **I**ntermediate-**S**cale **Q**uantum
- <200 qubits
- .1-1% gate error; transistor 1e-15 error
- Noisy machines you can sample from but not control well



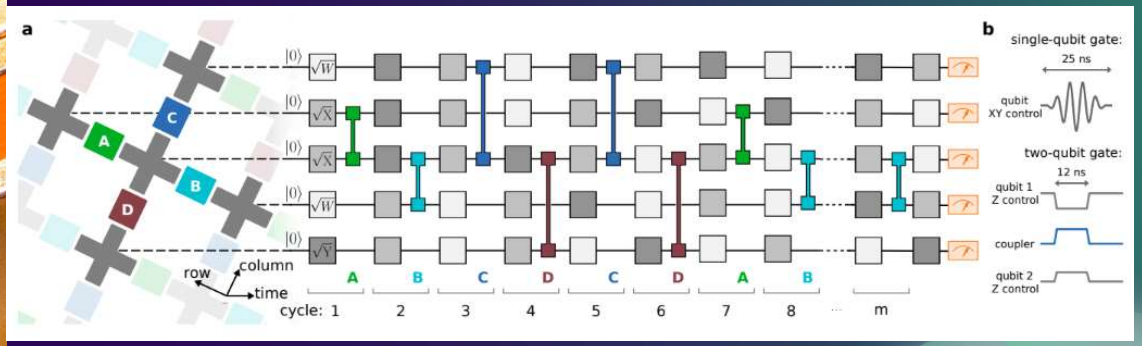
QED·C

Quantum Supremacy – Google, 2019

53 Qubits, 1% gate error



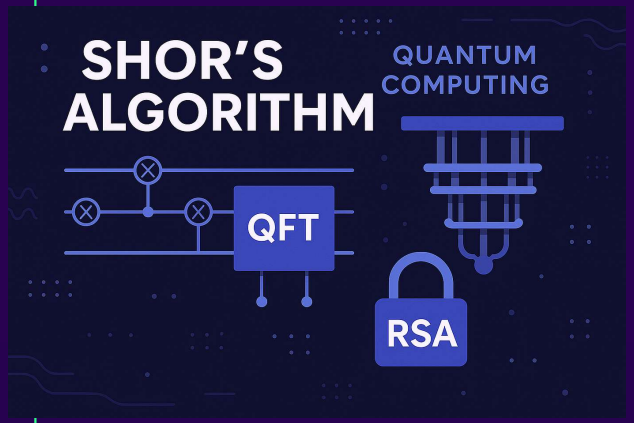
Random Circuit Sampling



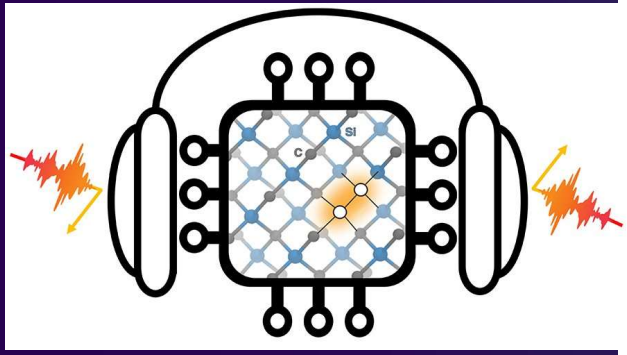
"It would take the world's best supercomputer 10,000 years to run this [useless] algorithm" (later debunked)

QED·C

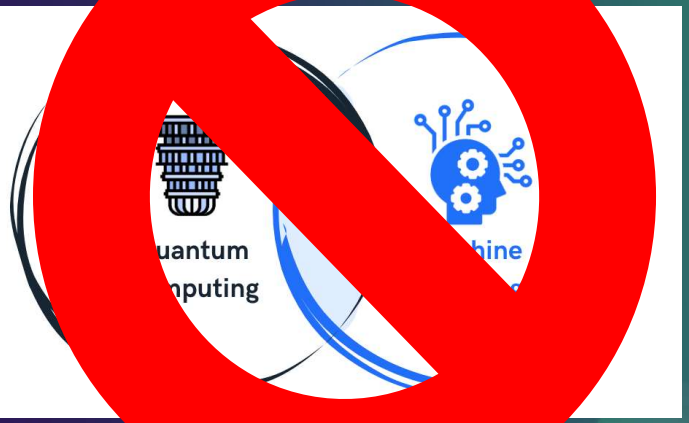
Quantum Algorithms



QSIM

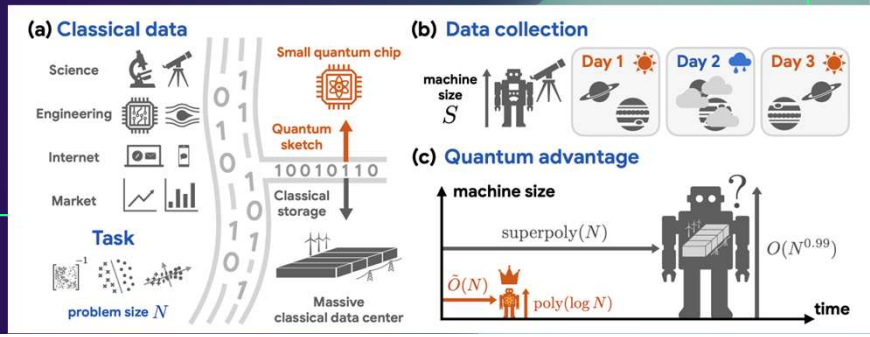


QML



Q-Day

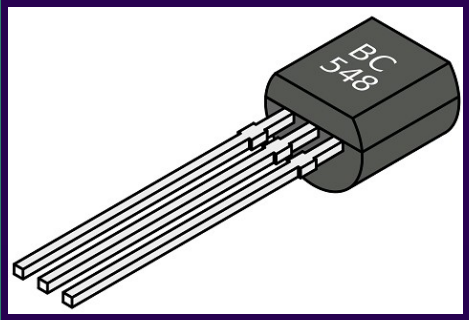
Need error rates $\sim 10^{-10}$

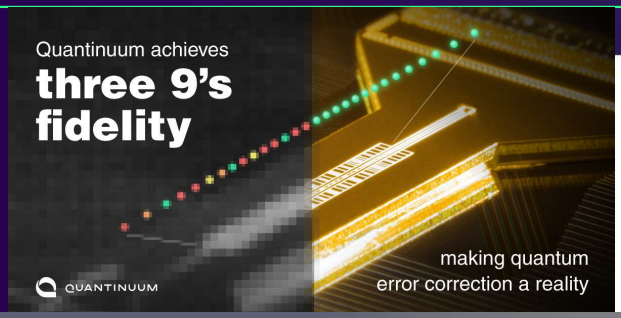


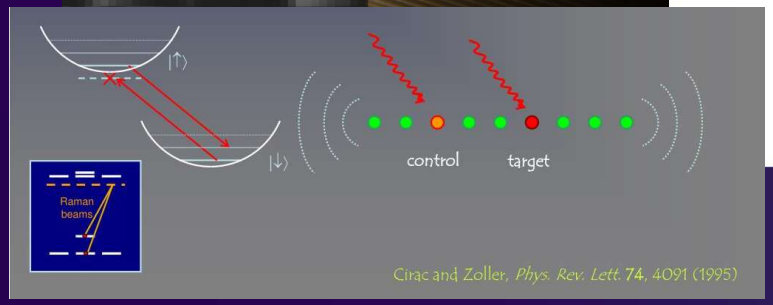
QED·C

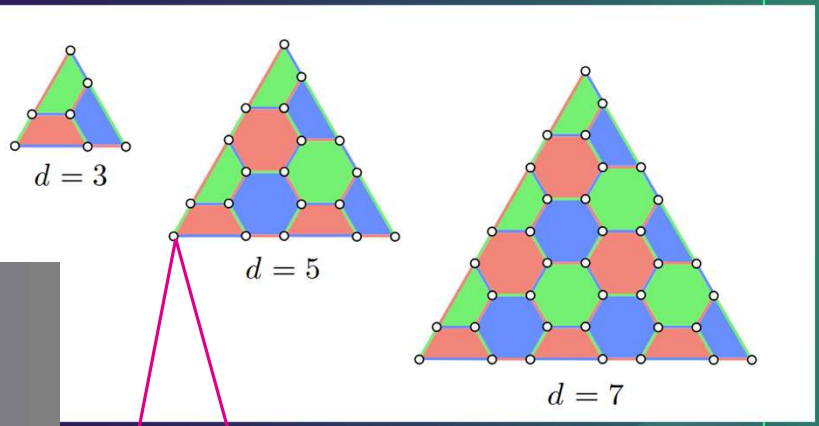
Logical Qubits/QEC

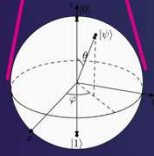
$p_{thresh} \sim 10^{-2}$ $n_{qubits} \sim d^2$









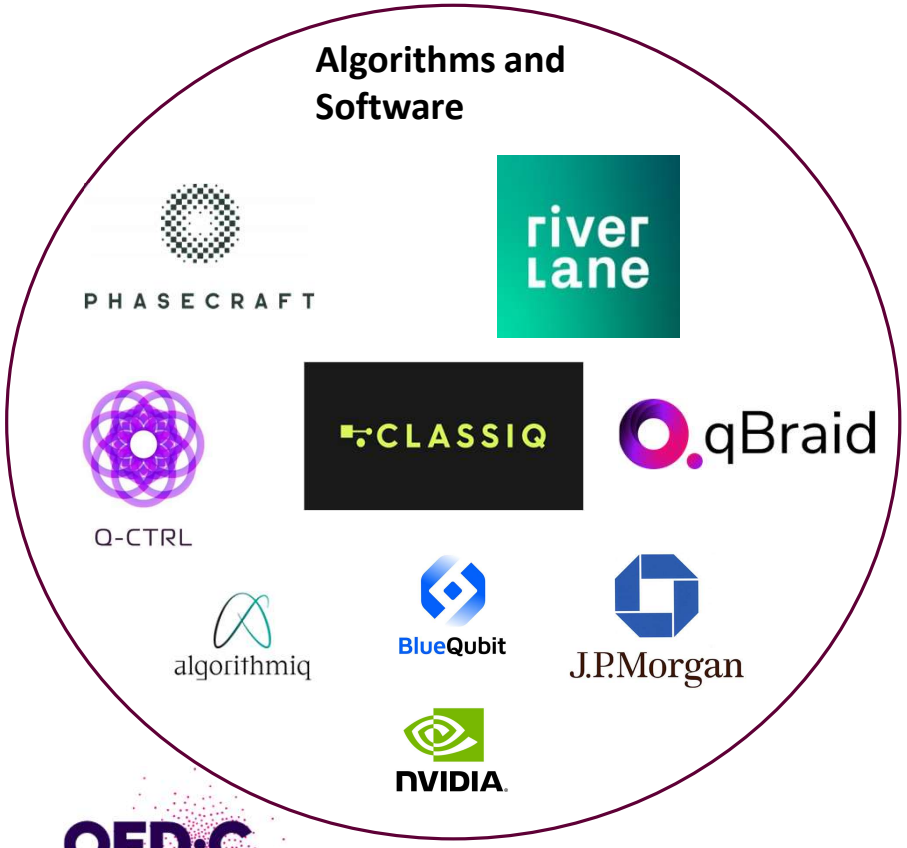


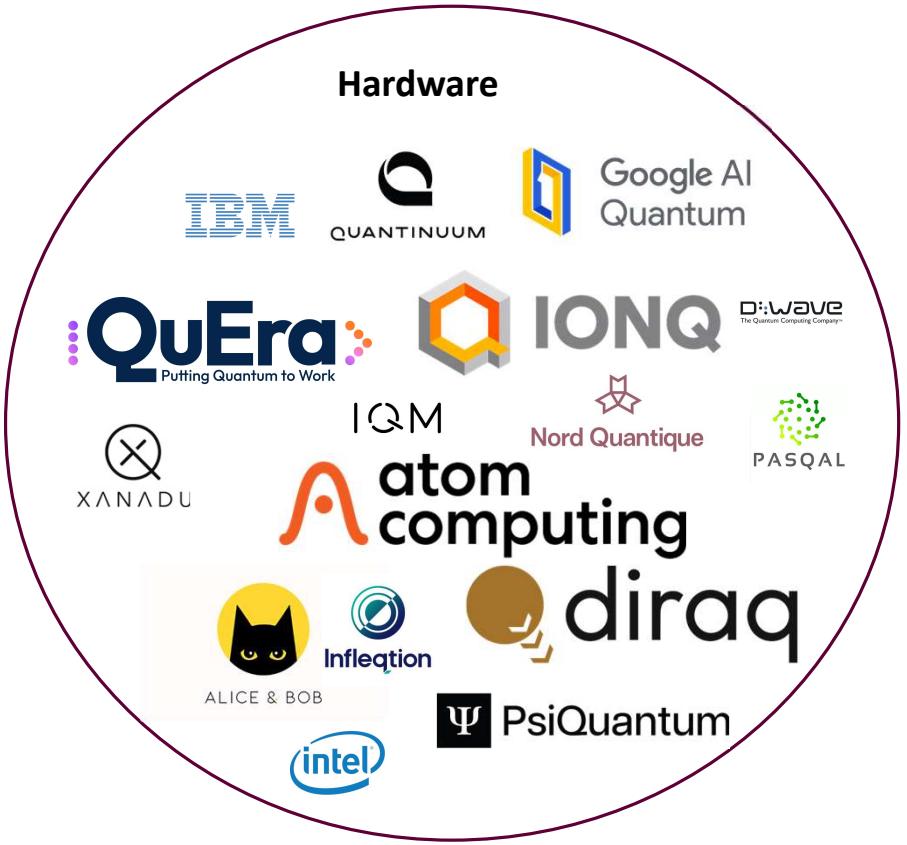
Error Rate $\sim 10^{-15}$ Error Rate $\sim 10^{-3}$ Error Rate $\sim \left(\frac{p_{err}}{p_{thresh}}\right)^{\frac{d+1}{2}}$

QED·C

Threshold Theorem

The Quantum Industry Today





QED·C

Oratomic

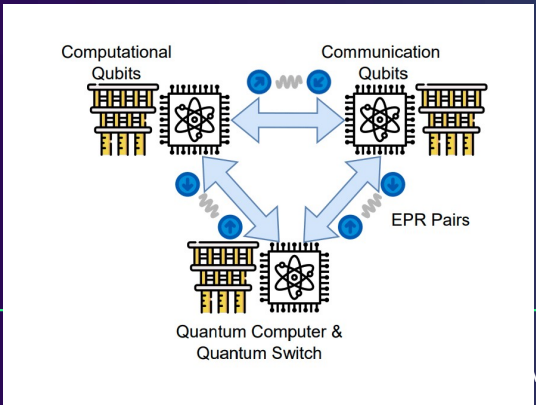
State of the Art

- 300 physical qubits
- 1e-3 gate error rate
- Efficient magic state distillation (cultivation)
- …not on the same platform (QuEra vs Quantinuum vs Google)
- If we could do all 3 together we could perform a 1 qubit quantum algorithm (useful quantum algorithm ~80 qubits)

QED·C

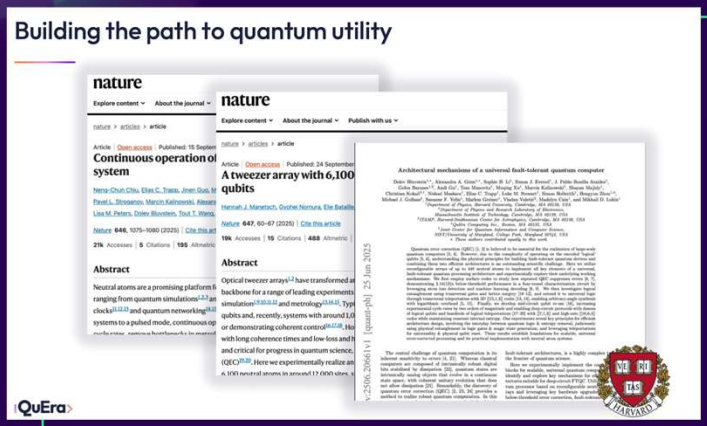
Distributed Quantum Computing

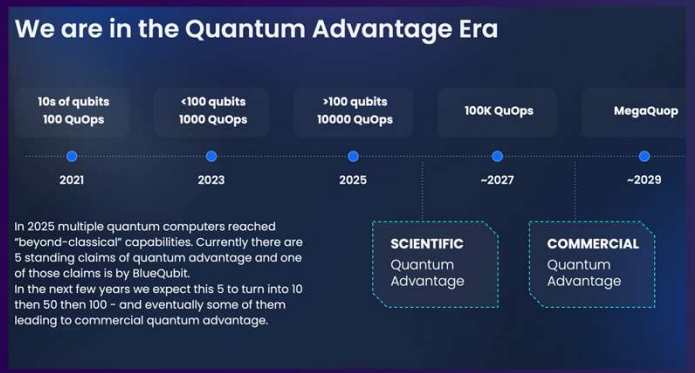
- Quantum Computers are not large enough today to run full optimized, error-corrected quantum algorithms
- But, if you networked them using quantum photonics, you might have a large enough distributed quantum computer (similar to distributed classical computing workloads in a datacenter for compute-intensive problems)
- This hasn't been demonstrated at scale but is a key part of several companies' roadmaps toward quantum advantage

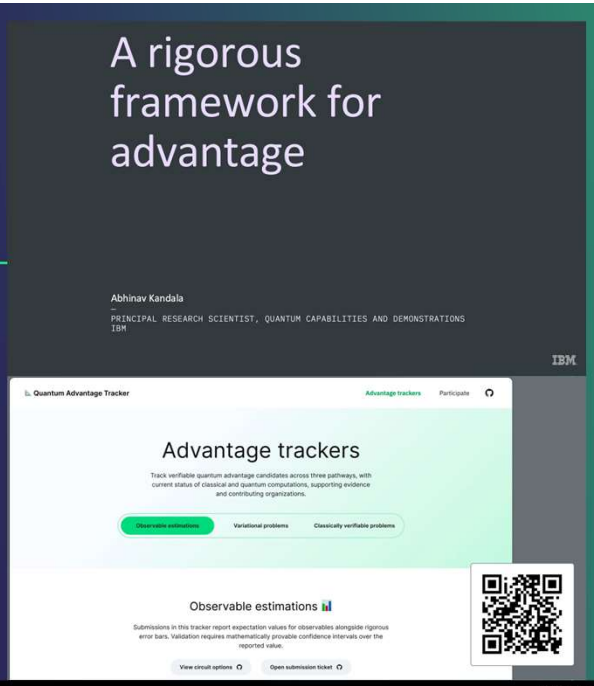


What is Quantum Advantage?

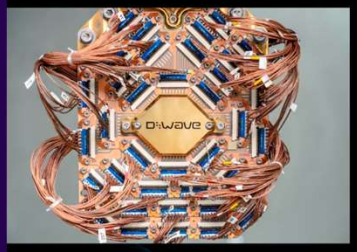
Previous QED-C Presentations







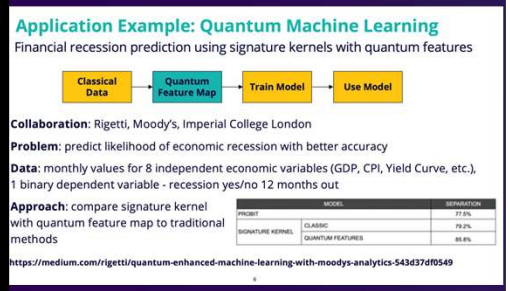
Quantum Milestones

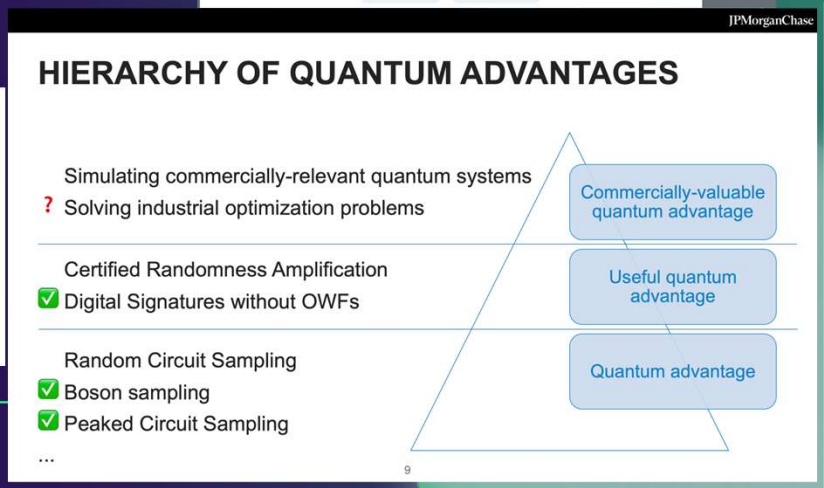


Supremacy: QPU can do a task that is *not feasible* using the most powerful classical platforms

Advantage: QPU routinely outperforms reasonable classical approaches in *application-relevant* test scenarios

Utility: Customers find outcomes that improve their bottom line: increase income or reduce costs





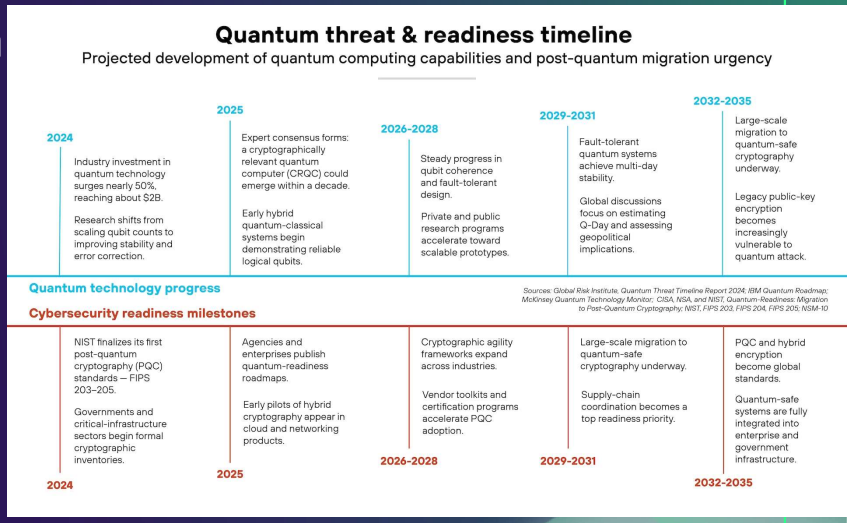
QED·C

What is Quantum Advantage?

- Many definitions and perspectives, no consensus
- Central question: how will we know we have hit quantum advantage?
  - Option A: When we can prove it mathematically
  - Option B: When we can sell commercial quantum computing services
  - Option C: When we have a useful application where we beat the current best-known classical algorithms
  - Option D: When someone forges all our private keys
- Let's examine Option D aka Q-Day

Q-Day

- The “day” when quantum computers can break a large enough cryptographic primitive (e.g. RSA2048) to cause cybersecurity impact
- PQC Algorithms (unlike RSA) assumed safe
- No proof of security. Quite possible some or all PQC candidates broken by QC
- If/when this happens, the impact will be immediate – no quibbling over definitions, will be a transformative moment in cybersecurity
- What can we do about it?



Source: Palo alto networks

Algorithmic vs Physical Encryption

Encryption type	Security Properties	Overhead	Implementation	Use Cases	Attacks
Algorithmic (RSA – encryption based on difficulty of factoring a product of primes)	Strong (unconditional assuming hardness of some computational problem)	High – compute intensive	Simple, done at data layer	Almost every encryption/key exchange in the world	Quantum attacks – require a "cryptographically-relevant" quantum computer
Physical (Spread Spectrum – encryption based on spreading signals over a wide frequency band)	Medium (nothing stopping an eavesdropper from guessing the right frequencies except technical difficulty)	High – bespoke hardware overhead	Complex, requires specific hardware implementations	Military, tactical networks, RF comms	RF signal interception – difficult but possible
Quantum (Quantum Key Distribution – physical encoding with added quantum security properties)	Unconditional or very strong (entanglement-based QKD is truly unconditionally secure, other implementations may have vulnerabilities)	Very high – bespoke hardware and nonstandardized algorithm implementation	Very complex, requires highly sensitive bespoke hardware	Mostly banks or ultra-secure networks	For unentangled - physical layer eavesdropping (photon number splitting attack, detector blinding attack, etc.)

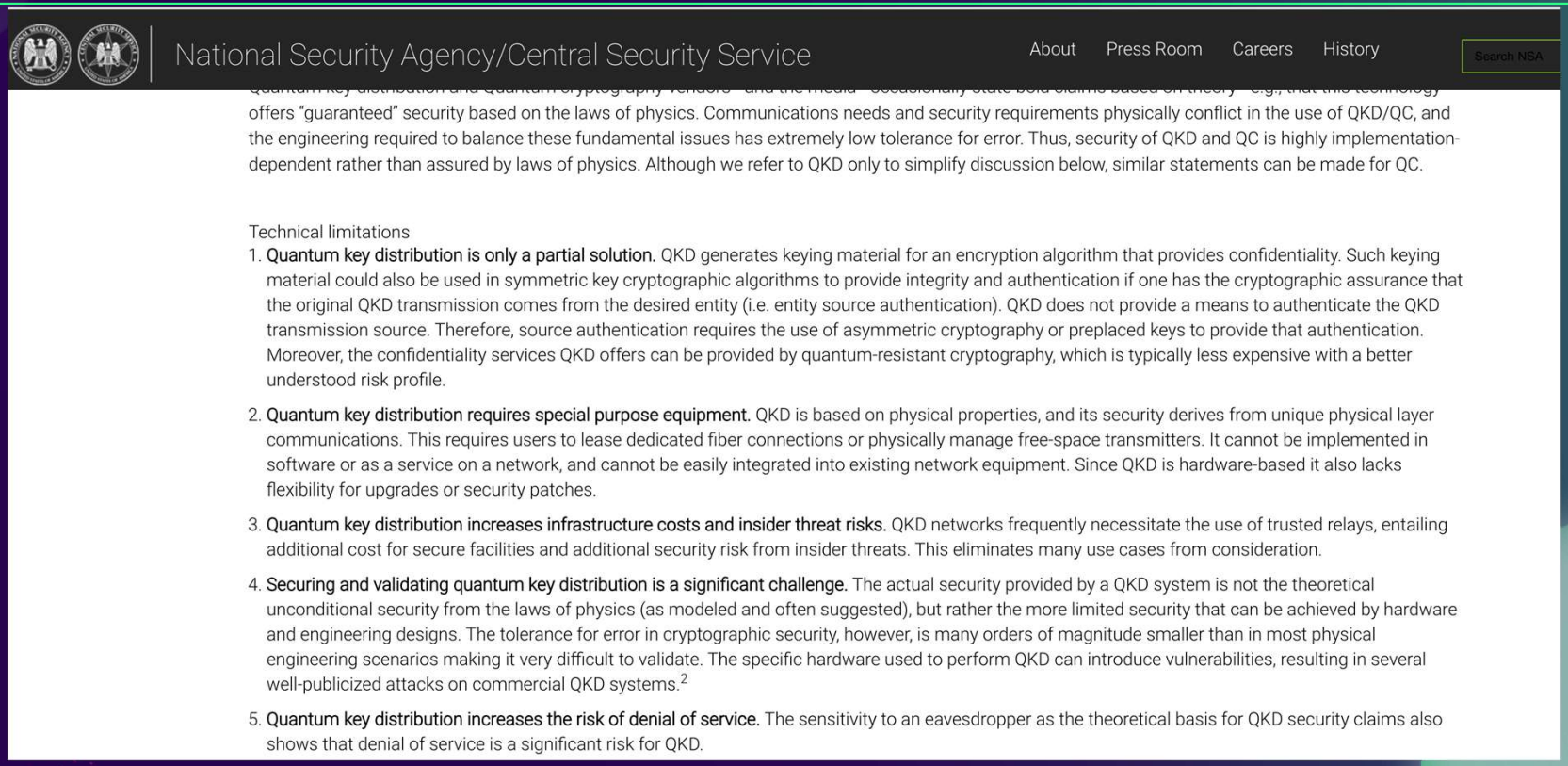
Quantum Networking Advantage

- Quantum Networking provides a key advantage (no pun intended) for securing cryptographic systems via Quantum Key Distribution (QKD):
  - Some people will say keys are unconditionally secure by no-cloning theorem. Don't believe this without examination!!
  - There are hundreds of side-channel attacks such as imperfect quantum cloning, photon number splitting, etc.
  - You can (with great difficulty) write a security proof for a specific implementation of a QKD system
  - Keys generated by entangled quantum systems can be proven unconditionally secure much more easily
- Provably secure quantum cryptography is still really difficult in practice due mainly to loss in fiber optic channels

Alternative Quantum Approaches

- QKD is not the only method of secure quantum comms:
- Quantum-secure direct communication (QSDC) – instead of generating keying material, transmit data bits directly with physical layer security provided by entanglement
- Quantum computational key generation – Use timing constraints and exponential quantum computing speedup to create security. Really exciting recent idea! https://arxiv.org/pdf/2602.04859v1
- Crypto-agility is very important!

Issues with Quantum Secure Comms



National Security Agency/Central Security Service

About Press Room Careers History Search NSA

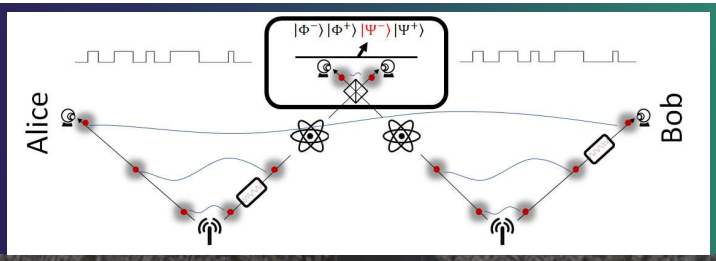
[illegible] offers "guaranteed" security based on the laws of physics. Communications needs and security requirements physically conflict in the use of QKD/QC, and the engineering required to balance these fundamental issues has extremely low tolerance for error. Thus, security of QKD and QC is highly implementation-dependent rather than assured by laws of physics. Although we refer to QKD only to simplify discussion below, similar statements can be made for QC.

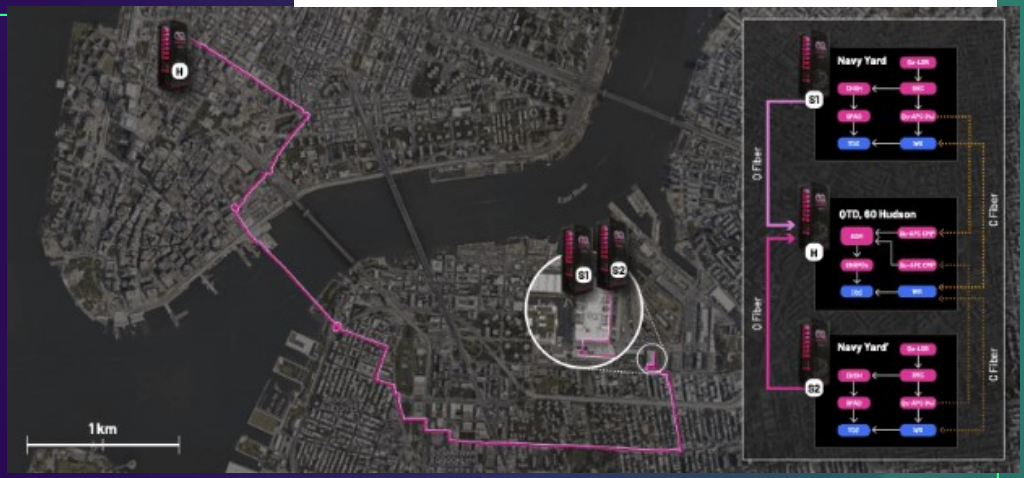
Technical limitations

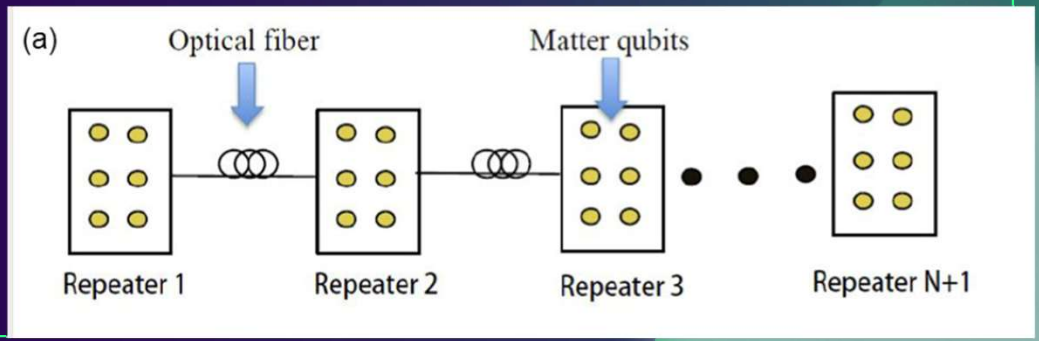
1. **Quantum key distribution is only a partial solution.** QKD generates keying material for an encryption algorithm that provides confidentiality. Such keying material could also be used in symmetric key cryptographic algorithms to provide integrity and authentication if one has the cryptographic assurance that the original QKD transmission comes from the desired entity (i.e. entity source authentication). QKD does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys to provide that authentication. Moreover, the confidentiality services QKD offers can be provided by quantum-resistant cryptography, which is typically less expensive with a better understood risk profile.
2. **Quantum key distribution requires special purpose equipment.** QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network, and cannot be easily integrated into existing network equipment. Since QKD is hardware-based it also lacks flexibility for upgrades or security patches.
3. **Quantum key distribution increases infrastructure costs and insider threat risks.** QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration.
4. **Securing and validating quantum key distribution is a significant challenge.** The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics (as modeled and often suggested), but rather the more limited security that can be achieved by hardware and engineering designs. The tolerance for error in cryptographic security, however, is many orders of magnitude smaller than in most physical engineering scenarios making it very difficult to validate. The specific hardware used to perform QKD can introduce vulnerabilities, resulting in several well-publicized attacks on commercial QKD systems.[2]
5. **Quantum key distribution increases the risk of denial of service.** The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD.

Quantum Repeaters

- Increase the fieldable distance of quantum communication solutions
- Still a fundamental loss limit of 3dB, aka 15km range
- Gen 1 (two-way) repeaters vs. Gen 2 (one-way) repeaters
- Recent exciting gen 1 experiment by Cisco and Qunnect in NYC
- No successful demonstrations of a gen 2 repeater to date







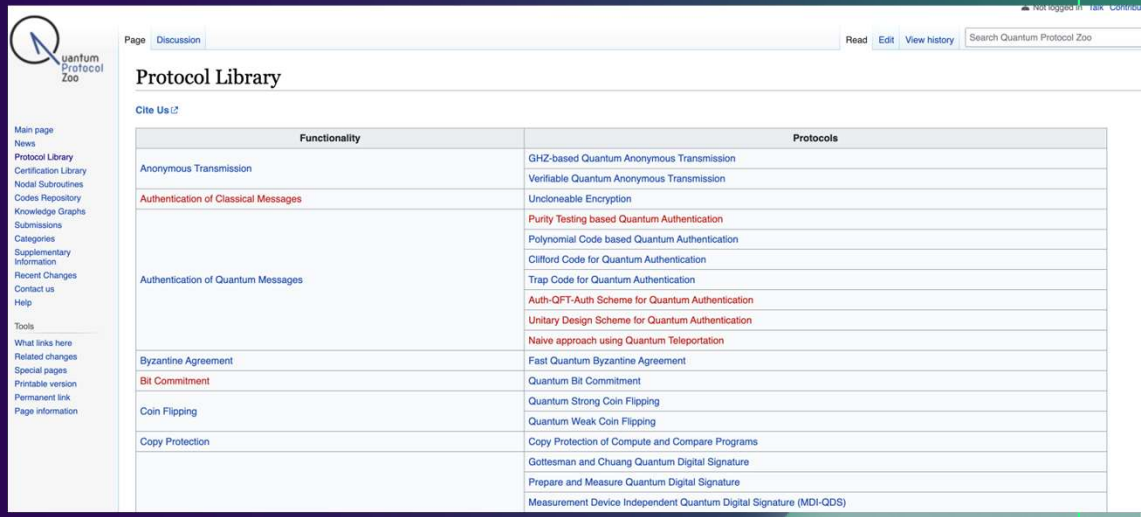
Quantum Space Networks

- Arguably the best way of getting around 3dB loss limit – go to space
- Free-space optical comms often more secure and less lossy than fiber optics
- Satellites are also a great way of generating remote entanglement via swapping in a centrally-accessible location

Source: AccessHub

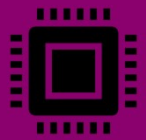
Quantum Networking advantage is really broad!

- Quantum networking advantage for security (QKD, QSDC, etc.)
- Quantum advantage in networking quantum devices (distributed quantum computing, distributed quantum sensing)
- Quantum decision advantage in networking classical devices (quantum Byzantine agreement, network nonlocality)
- All of these advantages are not complexity-theoretic – they enable fundamentally new applications, not just faster execution of the same computational tasks



Functionality	Protocols
Anonymous Transmission	GHZ-based Quantum Anonymous Transmission
	Verifiable Quantum Anonymous Transmission
Authentication of Classical Messages	Uncloneable Encryption
Authentication of Quantum Messages	Purity Testing based Quantum Authentication
	Polynomial Code based Quantum Authentication
	Clifford Code for Quantum Authentication
	Trap Code for Quantum Authentication
	Auth-QFT-Auth Scheme for Quantum Authentication
	Unitary Design Scheme for Quantum Authentication
	Naive approach using Quantum Teleportation
Byzantine Agreement	Fast Quantum Byzantine Agreement
Bit Commitment	Quantum Bit Commitment
Coin Flipping	Quantum Strong Coin Flipping
	Quantum Weak Coin Flipping
Copy Protection	Copy Protection of Compute and Compare Programs
	Gottesman and Chuang Quantum Digital Signature
	Prepare and Measure Quantum Digital Signature
	Measurement Device Independent Quantum Digital Signature (MDI-QDS)

What is Quantum Advantage? Take Two



- Requires entanglement
- Many modalities (superconducting, atoms, ions, photonic, etc.)
- Fundamentally based on computational complexity and efficiency**

- Advantage achievable pre-error correction
- Error correction a key part of scaling
- Mutually enabling
- Leverages quantum information via entanglement

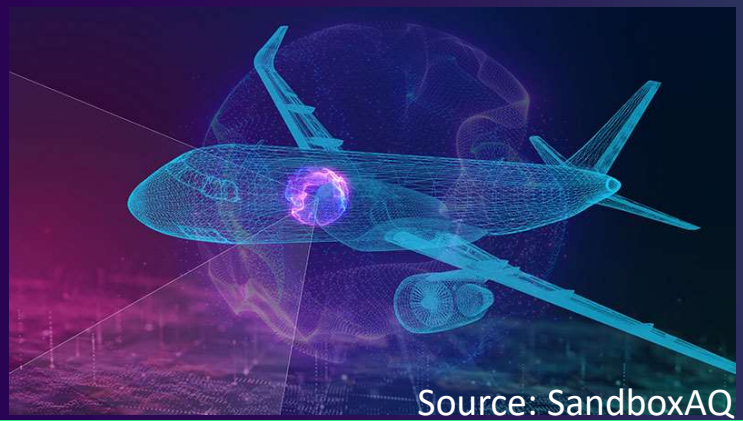
- Possible without entanglement (e.g. QKD)
- One modality (photonic)
- Enables fundamentally new applications

Quantum Sensing Advantage?

- Sensor performance today is largely very good
- It is possible to increase this performance by using atomic systems
- Are these quantum? Subject to debate
- If you use entanglement, you can get a sensing advantage that is truly "quantum", but this hasn't been demonstrated in an operationally useful way
- Competing on cost is a major challenge for quantum sensors

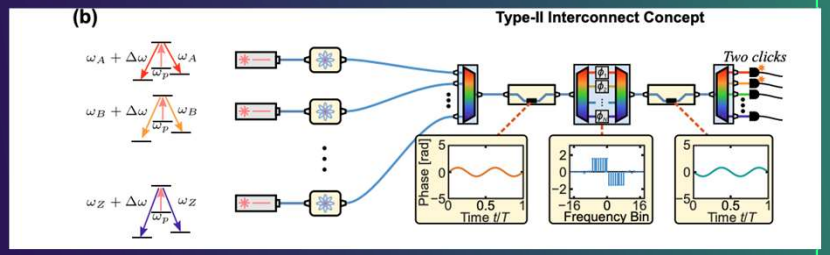
Example Application of Quantum Sensors

- Magnetic Naviation (Magnav) – in GPS-denied environments, the sensitivity of quantum magnetic field sensors (100fT/√Hz) can be used to navigate using Earth's magnetic field as a reference
- Need very good maps of Earth's magnetic field, first demo in 2004
- Do not need entanglement

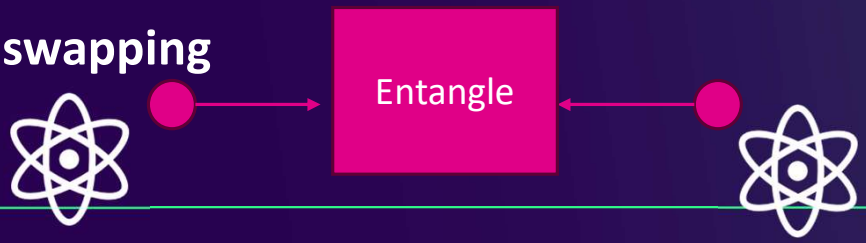


Source: SandboxAQ

What about entangled sensing?

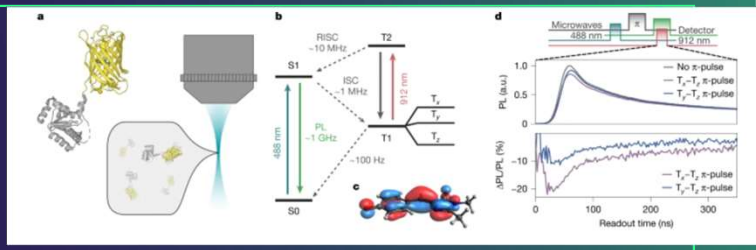


- Q: How do we entangle sensors?
- A: Quantum interconnect!
- Prepare two atoms in 0+1 states
- Atoms emit photons when they change energy. The energy of the photon is entangled with the energy of the atom
- Entangle those photons together and – like magic – the atoms themselves are entangled too!
- **Entanglement swapping**

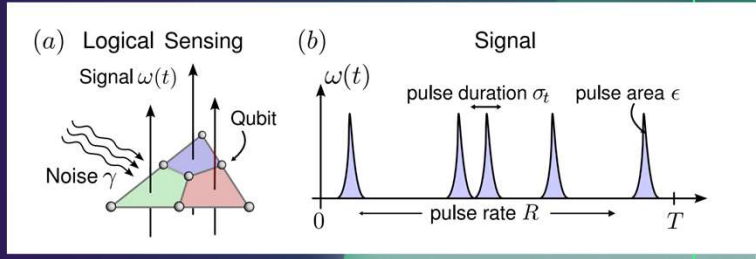


Entanglement and Sensing

- Entangled Quantum Sensing
  - Create Bell state of sensors: $|0_{S_1}\,0_{S_2}\rangle + |1_{S_1}\,1_{S_2}\rangle$ and measure independently
  - Sensitivity gap increases with the number of sensors (Fisher Information n^2 vs n)
  - Very far from demonstrating this with large n. Classical sensors are winning for now
- Error-corrected quantum sensing (large entangled error corrected state)
  - Could potentially provide an SNR advantage. Three key issues:
    - Error correction has barely been demonstrated today
    - A lot harder in a fielded quantum system – QCs are very isolated
    - Lots of no-go theorems on ECQS, but a few spaces might be possible such as “rare-event sensing”



Feder et al. 2025



Ott et al. 2026

Recap: Unanswered Questions

- When is a quantum communications protocol secure?
- What is quantum advantage?
- What is a logical qubit?
- What makes a sensor “quantum”?
- Need for standards and metrics around these technologies
- Companies may push back on standards that adversely affect their technologies, but the communication in this area is too fraught as it stands

Standards in Quantum

- Largely do not exist – mostly in the “definitions” stage
- Main technology that is standardized at this point is PQC, which has NIST standards resulting from a multiyear competition for new algorithms
- Not a quantum standard!!
- Several quantum standards making bodies: NIST, IEEE, ETSI, ISO/IEC, etc.
- Notably, the QED-C Standards TAC, while active in the standards and benchmarks space, is not itself a standards-making body

Standards Outlook within QED-C

- Standards and definitions around emerging technologies – quantum interconnects, distributed quantum computing, mid-circuit measurement, standards for quantum-hpc interfaces
- A lot of interest in standards and public communications surrounding quantum error correction codes (what is a logical qubit? How do we compare two implementations of a logical qubit?)

Where are standards going?

- I believe consensus on quantum advantage will solve a lot of these problems
- Once someone demonstrates a fault-tolerant quantum computation with clear quantum advantage, that will de facto set a standard for both quantum advantage and logical qubits
- Once Shor's algorithm can be executed (or PQC falls), quantum communication standards will naturally arise
- I don't think we will ever agree on what a quantum sensor is, we will just have sensors that are marketed as quantum – but may be wrong if entanglement-enhanced sensing ever makes it to market

Questions not on the radar yet

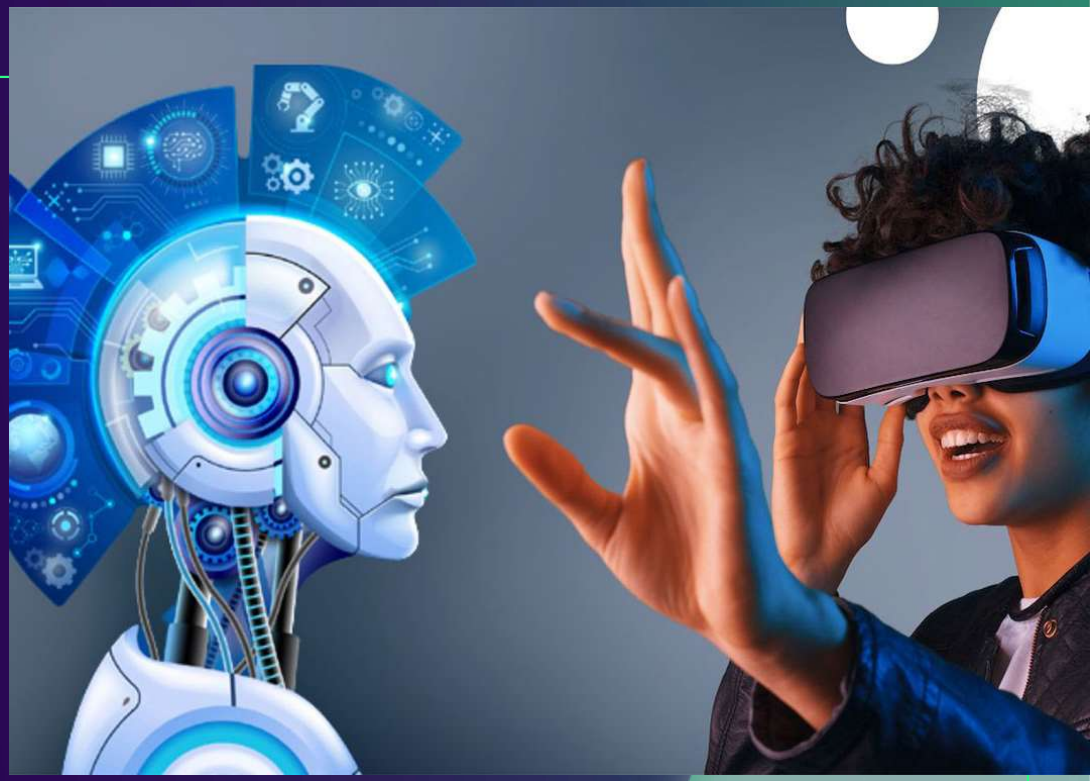
Quantum follows classical trends

- Information Theory -> Quantum Information Theory
- Bit -> Quantum Bit
- Transistor -> Quantum Transistor (logical qubit)
- Computer -> Quantum Computer
- Distributed network of computers -> Distributed QC
- Machine Learning -> Quantum Machine Learning
- Quantum must break free of this trend with something unique!

QED·C

The Next Trend: HCI

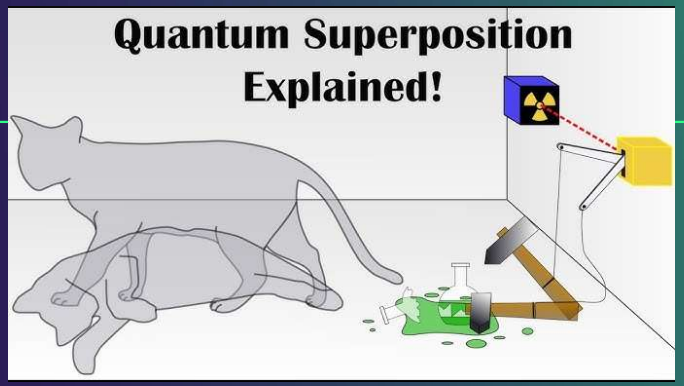
- To date, technology progress has been driven by fulfilling natural human functions more easily (Uber, Doordash, Cashapp)
- As AI becomes a bigger part of how we live our lives, we will integrate with it more tightly and start to reimagine our relationship with the digital world

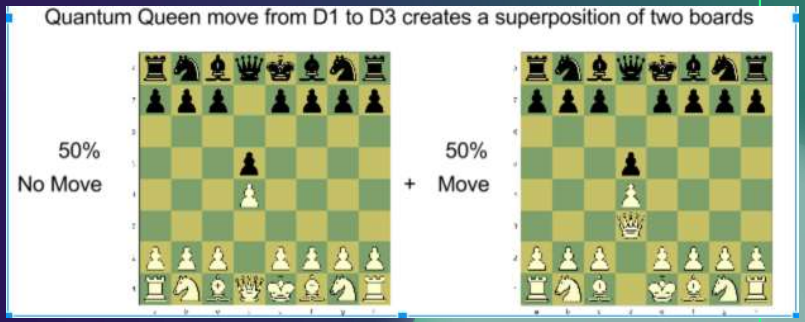


QED·C

Quantum HCI

- I believe that in 50 years, we will do many tasks in the digital world, and the way we think about these tasks will be quantum
- Starting point is natively probabilistic reasoning, then moving to quantum probabilistic reasoning
- More research needs to be done – what does a quantum-centric HCI look like?
- Check out quantum chess online





QED·C

Thank you for listening!