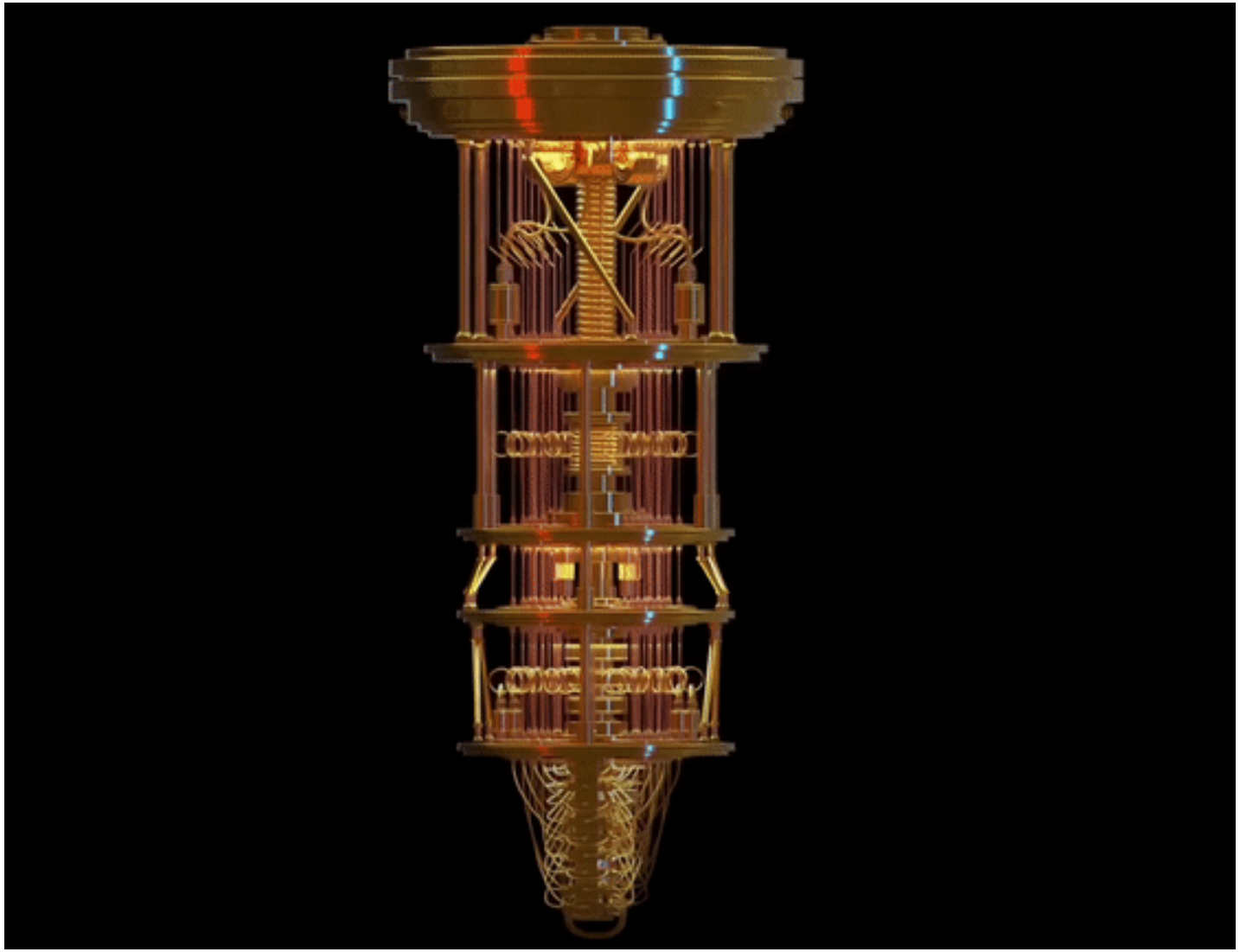
Current State of Quantum Computing



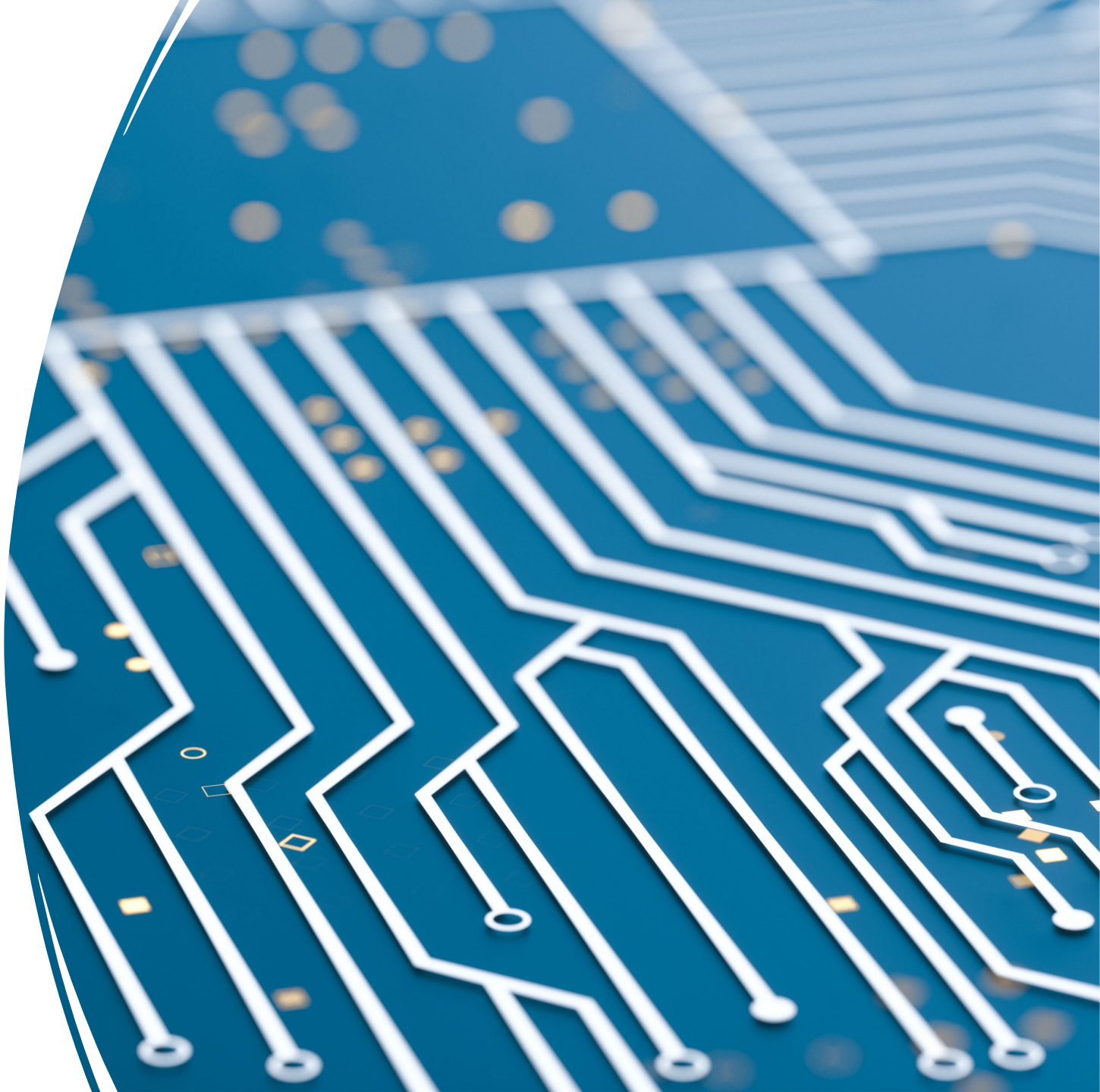
https://www.chuckeasttom.com/quantum.htm

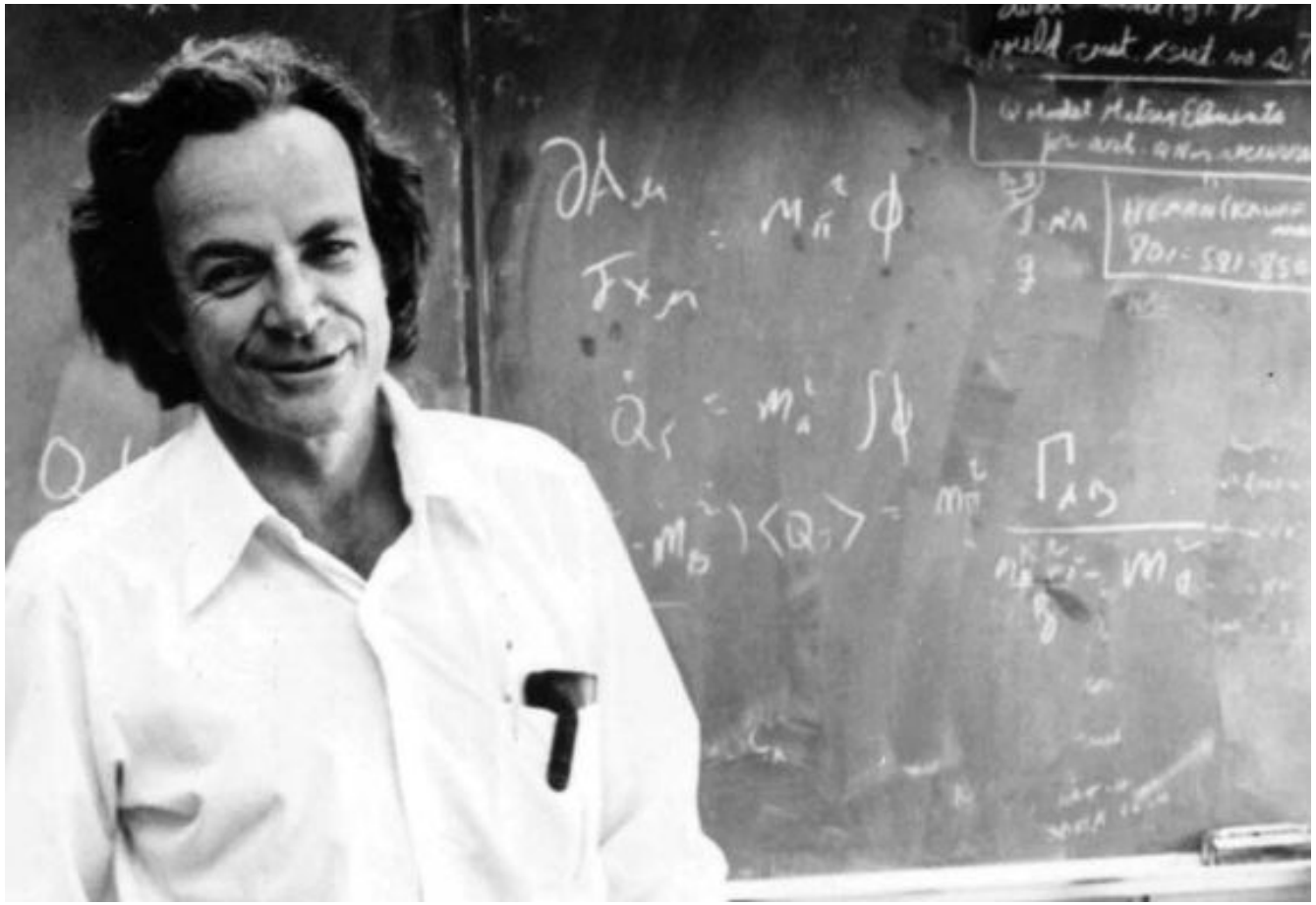
https://www.chuckeasttom.com/Current%20State%20of%20QC.pdf

Who Am I

- Ph.D. Computer Science, Ph.D. Nanotechnology, D.Sc. Cybersecurity
- Four masters (Systems Engineering, Defense Studies, Education, Applied Computer Science)
- 45 books
- 27 patents
- Member of the American Physical Society (Physics)
- Senior Member of the IEEE
- Member of American Institute of Aeronautics and Astronautics
- Member of the American Society for Quality (Aviation, Space, and Defense Division
- Adjunct professor for Vanderbilt and Georgetown

These slides are available at https://www.chuckeasttom.com/Current%20State%20of%20QC.pdf
Or
https://www.chuckeasttom.com/quantum.htm





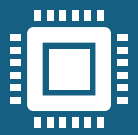
“The next reason that you might think you do not understand what I am telling you is, while I am describing to you how Nature works, you won’t understand why Nature works that way. But you see, nobody understands that. I can’t explain why Nature behaves in this peculiar way. Finally, there is this possibility: after I tell you something, you just can’t believe it. You can’t accept it. You don’t like it.”

- Richard Feynman

“I think I can safely say that nobody understands quantum mechanics” - Feynman

Some Misunderstandings -Quantum Computing – Quantum Supremacy

John Preskill coined the term quantum supremacy referring to a quantum computer solving a particular problem that is either unsolvable or extremely impractical to solve with a classical computer.



October 2019 Google and NASA performed calculations using the Sycamore quantum computer approximately 3 million times faster than can be done on the fastest classical computer.

Some Misunderstandings - Time Crystals

Researchers using Google's Sycamore quantum computer, verified their theoretical vision of a 'time crystal'. Crystals are made up of repeating units of atoms. A time crystal is a change that repeats through a system. Put more formally: a time crystal is a quantum system of particles whose lowest energy state is actually one in which the particles are in repetitive motion. Because this is the systems quantum ground state, it cannot lose energy and come to rest. These were first posited as theoretical constructs in 2012 by Nobel Laurate Dr. Frank Wilczek of MIT

https://www.sciencealert.com/physicists-used-a-quantum-computer-to-show-their-time-crystal-design-is-the-real-deal

In July 2022, researchers published their implementing a device-independent quantum key distribution (DIQKD) protocol that uses quantum entanglement. They were able to create two ions, about two meters apart that were in an entangled state.

https://www.nature.com/articles/s41586-022-04941-5

Quantum Networking With Drones

- In 2021, researchers in China used drones to create a small airborne quantum networking. In the prototype, the photons were sent just one kilometer "The work involved building a small laser-generating device and affixing it to one of the drones. As it fired, photons were split in two, creating entangled pairs. One of the paired photons was directed toward another drone while the other was directed to a ground station. The drone that received the entangled photon served only as a relay—after refocusing, the photon was forwarded to a third drone, which then sent it to a second ground station. Motorized devices were used on the drones to ensure transmitters and received lined up properly for transmission of the entangled photons."

- https://phys.org/news/2021-01-drones-local-quantum-networks.html

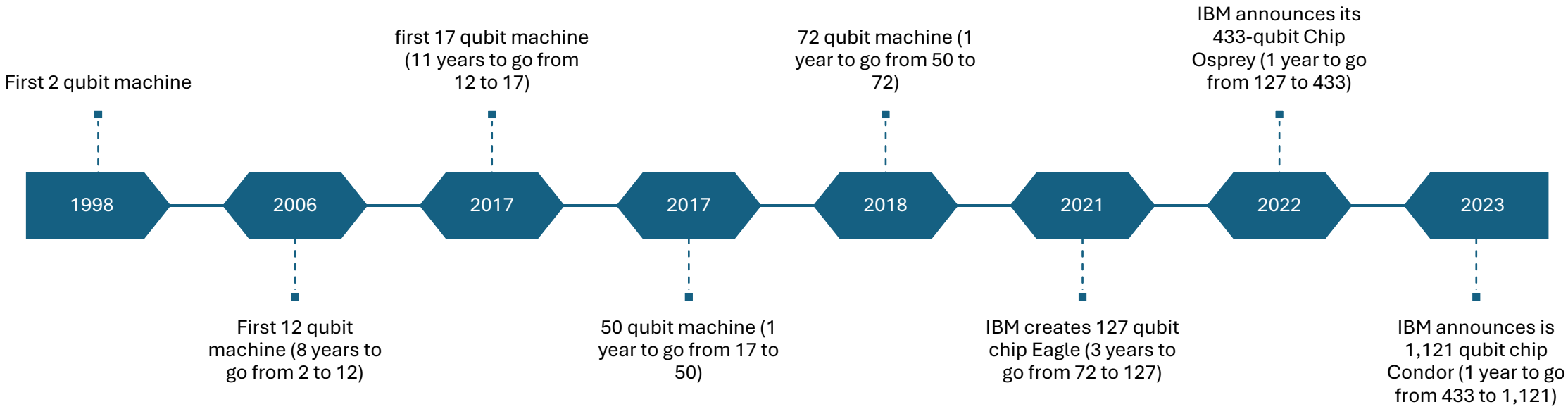
- https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.126.020503

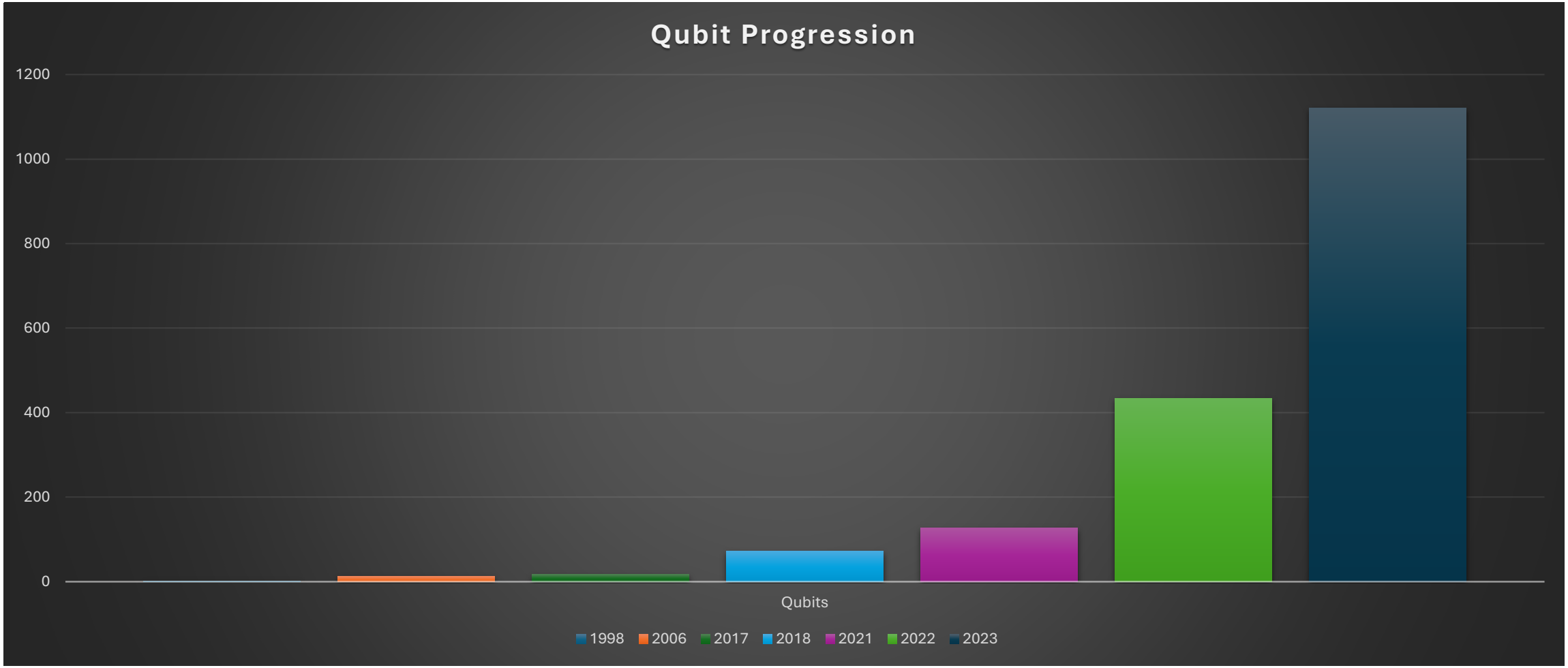
Quantum Networking with Global Navigation Satellite

Experimental exchange of single photons from Global Navigation Satellite System at a slant distance of 20000 kilometers, by exploiting the retroreflector array mounted on GLONASS satellites.

- https://arxiv.org/pdf/1804.05022.pdf

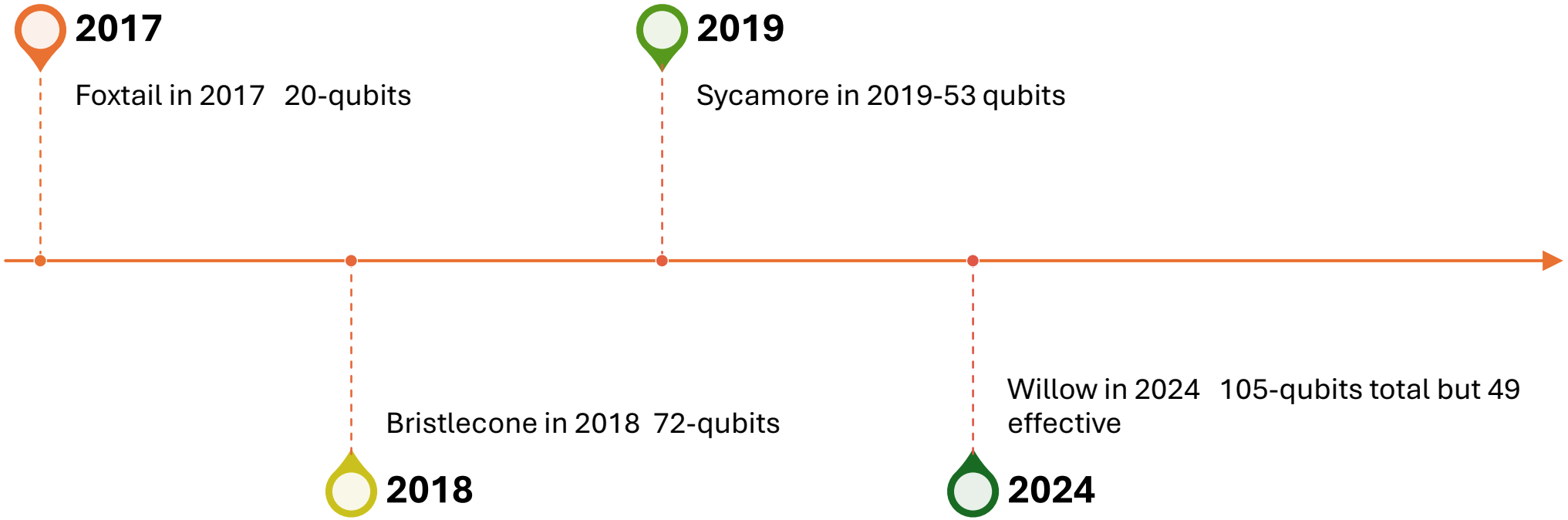
Quantum Computing Timeline – What is the trend





Quantum Computing Timeline – What is the trend

Googles Processors



Quantum Metrics

- Quantum volume is a metric measuring error rates in quantum computers. It expresses the maximum size of square quantum circuits that can be implemented successfully. In April 2022 Quantinuum (Previously Honeywell) has a 12-qubit system with a volume of 4096 or 12 X 12
- CLOPS (Circuit Layer Operations Per Second) is calculated as M × K × S × D / time taken where: M = number of templates = 100; K = number of parameter updates = 10; S = number of shots = 100 (or 1000); and D = number of QV layers = log2 QV.

Current exciting trends

- 30 June 2024 – Researchers from Oxford University successfully linked two quantum processors via an optical fiber network, enabling distributed quantum computing by demonstrating quantum entanglement between distant qubits, paving the way for scalable modular quantum computers and the development of a quantum internet
- 9 December 2024 – Google Quantum AI announced Willow, the first quantum processor where error-corrected qubits get exponentially better as they get bigger.
- 19 February 2025 – Microsoft announced Majorana 1, the first quantum processing unit based on a topological core

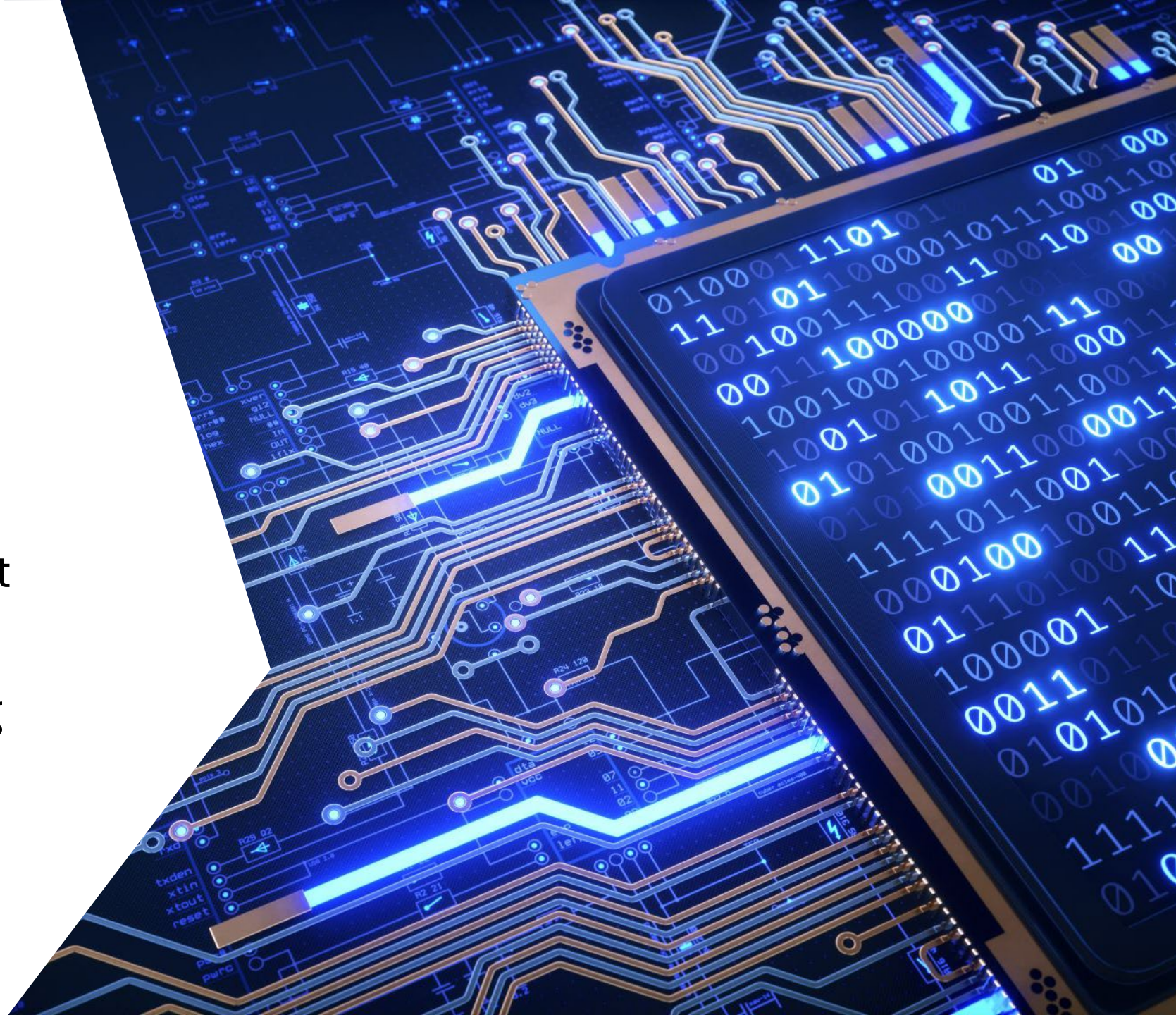
IBM Osprey

- At the Quantum Computing Summit on November 9th IBM announced the 433 Qubit OSPREY. The control electronics run in a cryo-CMOS controller chip that operates at approximately 4K. Rather than the 100 watts per qubit they previously needed, the new control chip uses only 10 milliwatts per qubit.

- IBM uses a quantum computing speed metric known as circuit layer operations per second (CLOPS), the company has gone from 1,400 to 15,000 CLOPS with its best systems.

IBM Condor

- December 2023
- A 1,121 superconducting qubit quantum processor
- A 50% increase in qubit density and over a mile of high-density cryogenic flex IO wiring within a single dilution refrigerator.



Atom Computing

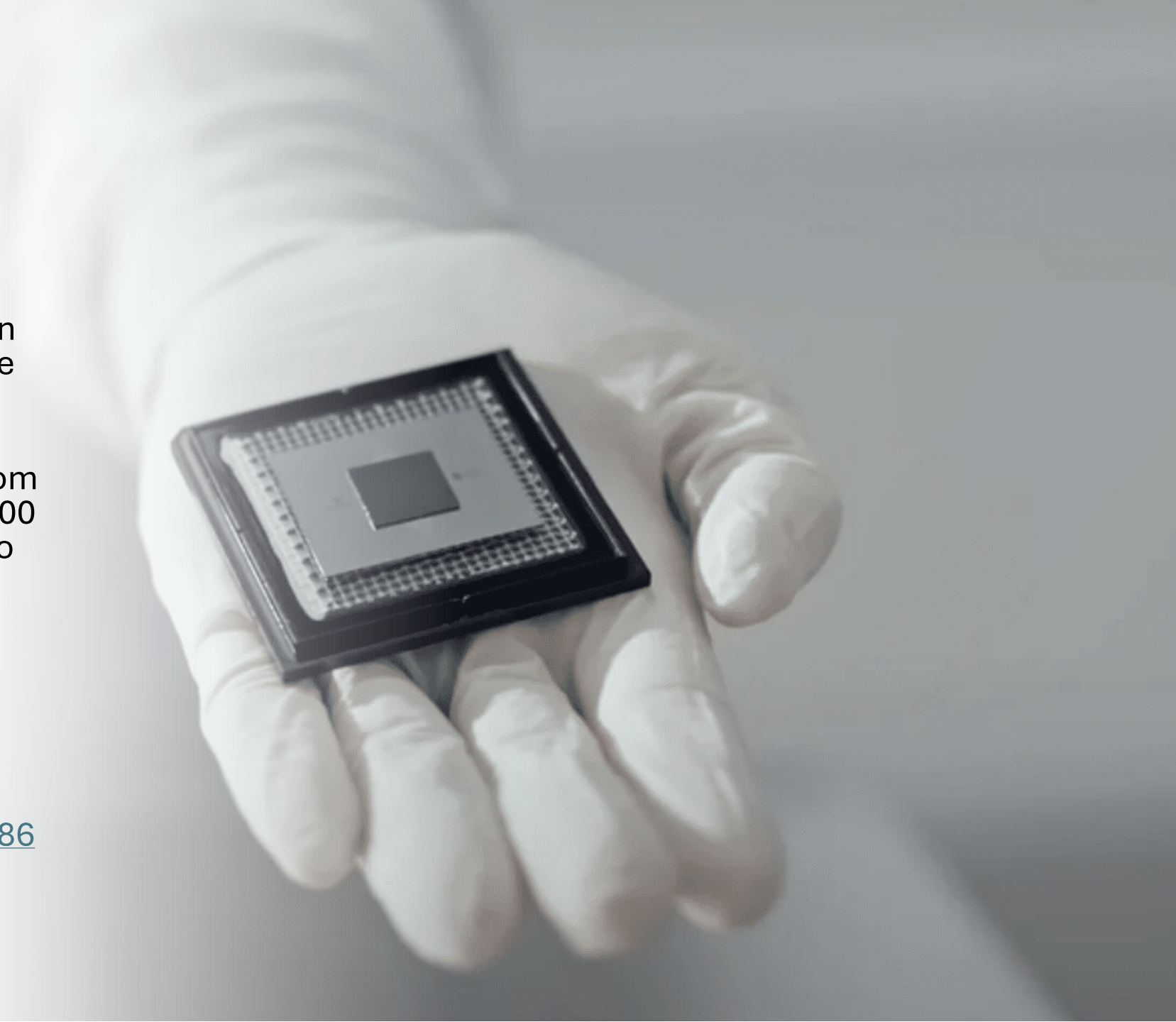
Atom Computing announces that it has "created a 1,225-site atomic array, currently populated with 1,180 qubits“ based on Rydberg atoms. Rydberg atoms are highly excited atoms with one or more electrons in high principal quantum number states, meaning their outermost electron is in a state with a high energy level (large n, where n is the principal quantum number). These atoms exhibit unique properties due to the large distance between the nucleus and the excited electron.

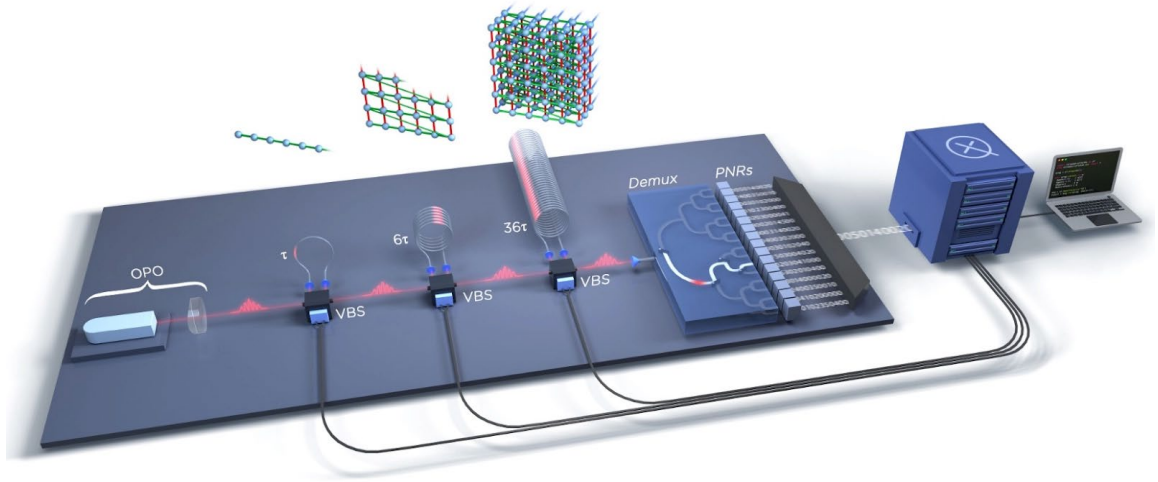
Willow Chip

Announced in December of 2024. The most important issue is that Willow can reduce errors exponentially as we scale up using *more* qubits. The more qubits the fewer error.

Willow improved T1 coherence time from the 20 microseconds of Sycamore to 100 microseconds. T1 coherence time, also known as the longitudinal relaxation time, refers to the time it takes for a quantum system (such as a qubit in quantum computing) to return to its thermal equilibrium state after being disturbed.

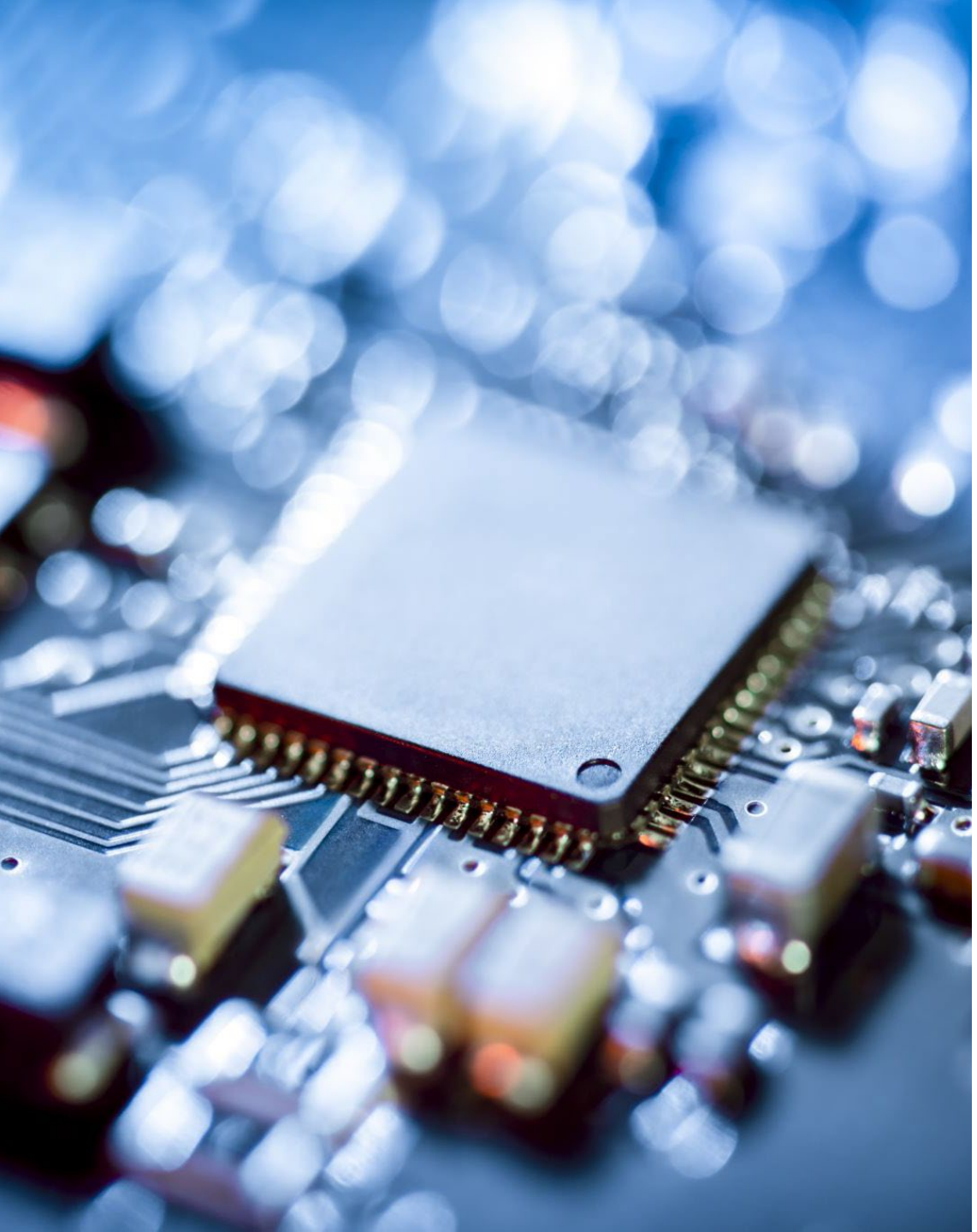
https://www.nature.com/articles/s41586-024-08449-y





Xanadu’s Borealis processor

216 Qubits announced in 2022. This processor is a photonic based quantum processor. It is the first *photonic* quantum computer with quantum computational advantage to offer users full programmability over all its gates — over 1200 parameters can be freely specified by the user encoding their program, as well as the brightness of the input squeezed-state qubits



China's Jiuzhang

The Jiuzhang processor, also known as the "Light-Matter Interactions Enhanced by Quantum Decoherence" processor, is a photonic quantum computing device developed by a team of researchers in China. It gained significant attention in 2020 due to claims of achieving quantum supremacy, which refers to the ability of a quantum computer to solve certain problems faster than classical computers.

The latest version of Jiuzhang, as of 2024, is the Jiuzhang 3.0 which has 255 detected photons. The original Jiuzhang had 76 and Jiuzhang 2.0 had 113.

Xiaohong

504 qubit processor developed in partnership with the Chinese Academy of Sciences and QuantumCTek. This was released in 2024 and is a superconducting chip.

Top 5 Processors

Rank	System (vendor)	Qubits	Architecture	Year announced / status	Notes
1	**Atom Computing platform**	**~1,180 populated sites (1,225 available)**	Neutral-atom (gate-based)	Oct 2023 (prototype)	First universal, gate-based system to exceed 1,000 qubits; array of 1,225 sites with ~1,180 atoms loaded.
2	**IBM “Condor”**	**1,121**	Superconducting transmons (gate-based)	Dec 2023 (announced; in IBM roadmap/system two)	First IBM chip to break 1,000 qubits.
3	**“Xiaohong” / Tianyan-504 (CAS/CTQG, China)**	**504**	Superconducting (gate-based)	Dec 2024 (announced)	China’s largest gate-model processor to date.
4	**IBM “Osprey”**	**433**	Superconducting transmons (gate-based)	Nov 2022 (announced)	Predecessor to Condor; still one of the largest gate-model chips.
5	**PASQAL (record neutral-atom device)**	**324 atoms**	Neutral-atom (analog/FPQA)	2022 (research milestone)	Record 324-atom processor reported with Institut d’Optique.

Caltech sets new record

September 24, 2025. Caltech physicists have created the largest qubit array ever assembled: 6,100 neutral-atom qubits trapped in a grid by lasers. Previous arrays of this kind contained only hundreds of qubits. The Caltech team led by Manuel Endres succeeded in trapping 6,100 neutral atoms (cesium atoms) configured as qubits in a 2D optical tweezer array — the largest qubit array of this type reported to date.

- Coherence (superposition lifetime) of about 12.6 seconds
- Single-qubit control/manipulation fidelity of ~99.98%

This is not yet a full universal quantum computer executing large-scale algorithms and full quantum error correction. The paper and reports emphasise: next steps are entanglement and error correction at scale. The qubit count is physical atoms trapped and controlled; it does *not* yet mean many logical qubits (error-corrected, fault-tolerant).

- https://www.caltech.edu/about/news/caltech-team-sets-record-with-6100-qubit-array

Amazon Ocelot

February 27, 2025

- Ocelot is a first-generation quantum computing chip developed by AWS in collaboration with the AWS Center for Quantum Computing at California Institute of Technology (Caltech). It is a *prototype* rather than a full-scale commercial quantum computer, AWS explicitly states it's an early step in their quantum hardware roadmap.

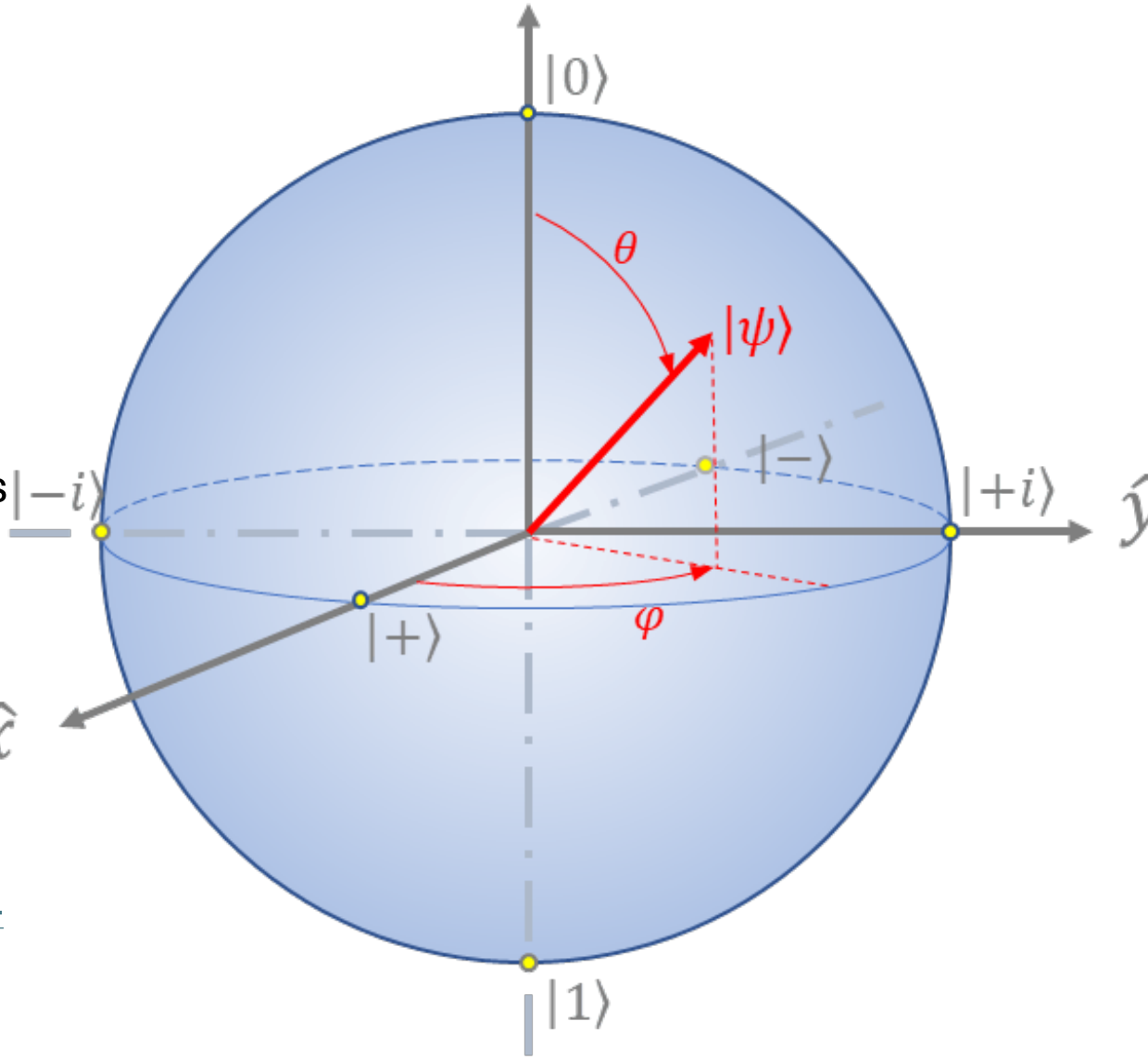
- The chip uses *superconducting quantum circuits* and an architecture built around something called "cat qubits" (bosonic qubits) for error correction. Cat qubits / Bosonic qubit architecture are qubits encoded in the states of an oscillator (a bosonic mode) rather than a simple two-state (0/1) physical qubit. The advantage: certain error types (in particular bit-flip errors) can be suppressed more naturally.
- The chip consists of two integrated silicon microchips (stacked) each roughly 1 cm^2 in area, with superconducting circuit elements (thin film of tantalum) used for the oscillators.
- The Ocelot has demonstrated bit-flip times approaching one second. AWS states that compared with "standard" quantum error correction schemes (e.g., surface codes), the Ocelot architecture might require as little as one-tenth the physical qubit resources.

Topological QC

- 19 February 2025– Microsoft announced Majorana 1, claiming to be the first qubit architecture based on a topological superconductor

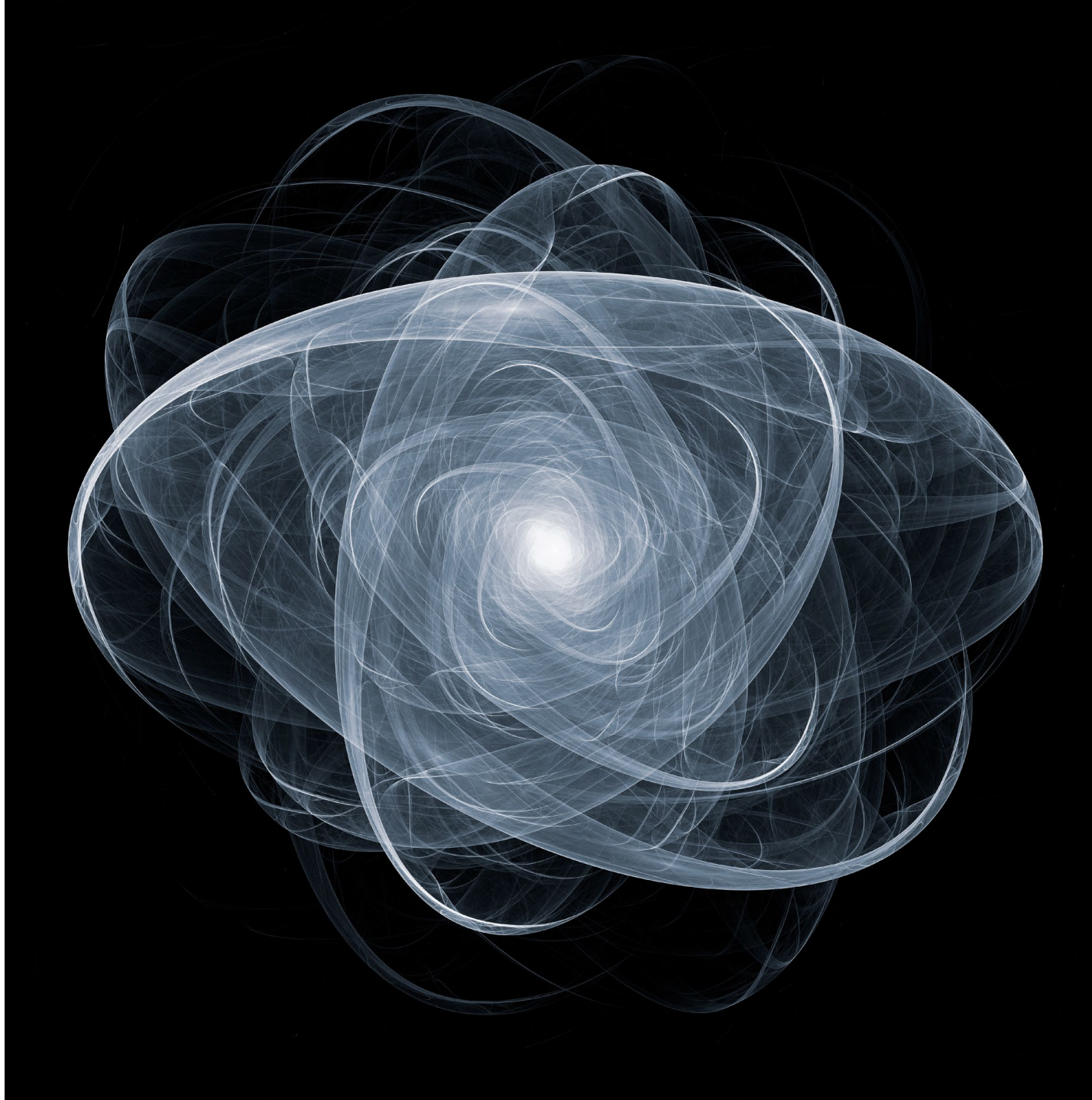
January 2025: MIT researchers in the Department of Physics, the Research Laboratory of Electronics (RLE), and the Department of Electrical Engineering and Computer Science (EECS) developed two new control techniques to achieve a world-record single-qubit fidelity of 99.998 percent. This result complements then-MIT researcher Leon Ding's demonstration last year of a 99.92 percent two-qubit gate fidelity.

https://news.mit.edu/2025/fast-control-methods-enable-record-setting-fidelity-superconducting-qubit-0114



February 2025: Infleqtion has created a 16×16 neutral atom array, the largest of its kind in the UK, as part of the Scalable *Quantum Atomic Lattice computing tEstbed (SQALE)* project. This 256 neutral atom array, developed at the National Quantum Computing Centre (NQCC) Harwell Campus, represents an advancement in scalable, fault-tolerant quantum computing using neutral atom platforms.

https://quantumcomputingreport.com/infleqtion-announces-reaching-a-256-neutral-atom-array-milestone-in-the-uk/



Recent Quantum News

May 18, 2025: Researchers from Yale University published in Nature created qudits—a quantum system that holds quantum information and can exist in more than two states. Using a qutrit (3-level quantum system) and a ququart (4-level quantum system), the researchers demonstrated the first-ever experimental quantum error correction for higher-dimensional quantum units using the Gottesman–Kitaev–Preskill (GKP) bosonic code.
https://phys.org/news/2025-05-successful-quantum-error-qudits.html

Quantum Applications

- Other than cracking cryptography
- Search Algorithms – Grovers algorithm
- AI/ML
- Drug Research
- Financial modeling
- Random Number generation

Quantum for Healthcare

- March 20, 2023, IBM and a clinic in Cleveland are working together to use quantum computing for healthcare research.
- https://www.sdxcentral.com/articles/news/ibm-cleveland-clinic-install-worlds-first-quantum-computer-for-health-care-research/2023/03/

Quantum Computing – NIST Round 3

Asymmetric Cryptography

- Classic McEliece
- CRYSTALS-KYBER
- NTRU
- SABER

Digital Signature

- CRYSTALS-DILITHIUM
- FALCON
- Rainbow

Alternate Public Key

- BIKE
- FrodoKEM
- HQC
- NTRU Prime
- SIKE

Alternate Digital Signature

- GeMSS
- Picnic
- SPHINCS+

Standards

The NIST Post-Quantum Cryptography (PQC) Standards are a set of cryptographic algorithms selected and standardized by the National Institute of Standards and Technology (NIST)

- CRYSTALS-KYBER for Public-key Encryption and Key-establishment Algorithms. Note, NIST is now referring to this algorithm as Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM).
- CRYSTALS-DILITHIUM for Digital Signatures
- FALCON for Digital Signatures
- SPHINCS+ for Digital Signatures

PKCS and Crystals Kyber

- PKCS #11 CRYSTALS-Kyber key operations can be performed in hardware or software.
  - PKCS #11 callable services that support CRYSTALS-Kyber key operations are: PKCS #11 Derive Key (CSFPDVK and CSFPDVK6)
  - PKCS #11 Generate Key Pair (CSFPGKP and CSFPGKP6)
  - PKCS #11 Get Attribute Value (CSFPGAV and CSFPGAV6)
  - PKCS #11 Set Attribute Value (CSFPSAV and CSFPSAV6)
  - PKCS #11 Token Record Create (CSFPTRC and CSFPTRC6)
- CCA callable services that support CRYSTALS-Kyber key operations are: ECC Diffie-Hellman (CSNDEDH and CSNFEDH)
  - PKA Encrypt (CSNDPKE and CSNFPKE)
  - PKA Decrypt (CSNDPKD and CSNFPKD)
  - PKA Key Generate (CSNDPKG and CSNFPKG)
  - PKA Key Import (CSNDPKI and CSNFPKI)
  - PKA Key Token Build (CSNDPKB and CSNFPKB)
  - PKA Key Token Change (CSNDKTC and CSNFKTC)
  - PKA Key Translate (CSNDPKT and CSNFPKT)
  - PKA Public Key Extract (CSNDPKX and CSNFPKX)

NIST Cryptography

FIPS 203 (ML-KEM or CRYSTALS-Kyber): This algorithm is designed for key establishment, ensuring that sensitive information can be securely exchanged, even in the presence of quantum-capable adversaries. It stands out for its efficiency in encryption and decryption, making it suitable for a wide range of applications, from secure communications to cloud storage. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf

FIPS 204 (ML-DSA or CRYSTALS-Dilithium): Targeting digital signatures, ML-DSA provides a robust mechanism for verifying identities and ensuring the integrity of messages and documents. Its balance of speed and security makes it a strong candidate for use in software updates, code signing, and any scenario where the authenticity of information is critical. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf

FIPS 205 (SLH-DSA or SPHINCS+): Also focused on digital signatures, SLH-DSA offers an alternative that emphasizes resilience against attacks, including those leveraging quantum computing. While it is slightly less efficient than ML-DSA, its stateless nature provides an additional layer of security, particularly for applications requiring long-term integrity. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf

Standards

- The National Security Agency has published the Commercial National Security Algorithm Suite 2.0 (NSA, 2024). This document identifies algorithms that can be used for National Security Systems (NSS). Many of the algorithms are the same found in FIPS and NIST standards.

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
ML-KEM (aka CRYSTALS-Kyber)	Asymmetric algorithm for key establishment	FIPS PUB 203	Use Category 5 parameter, ML-KEM-1024, for all classification levels.
ML-DSA (aka CRYSTALS-Dilithium)	Asymmetric algorithm for digital signatures in any use case, including signing firmware and software	FIPS PUB 204	Use Category 5 parameter, ML-DSA-87, for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. LMS SHA-256/192 is recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

Quantum Networking

In June 2017, Chinese physicists led by Pan Jianwei achieved a quantum entanglement record by measuring entangled photons over a distance of 1203 km between a satellite and two ground stations as part of the Quantum Experiments at Space Scale (QUESS) project. The experiment used the Micius satellite and was a major breakthrough for developing secure quantum communication networks. This satellite-based method was significantly more efficient for long-distance communication than using fiber optics

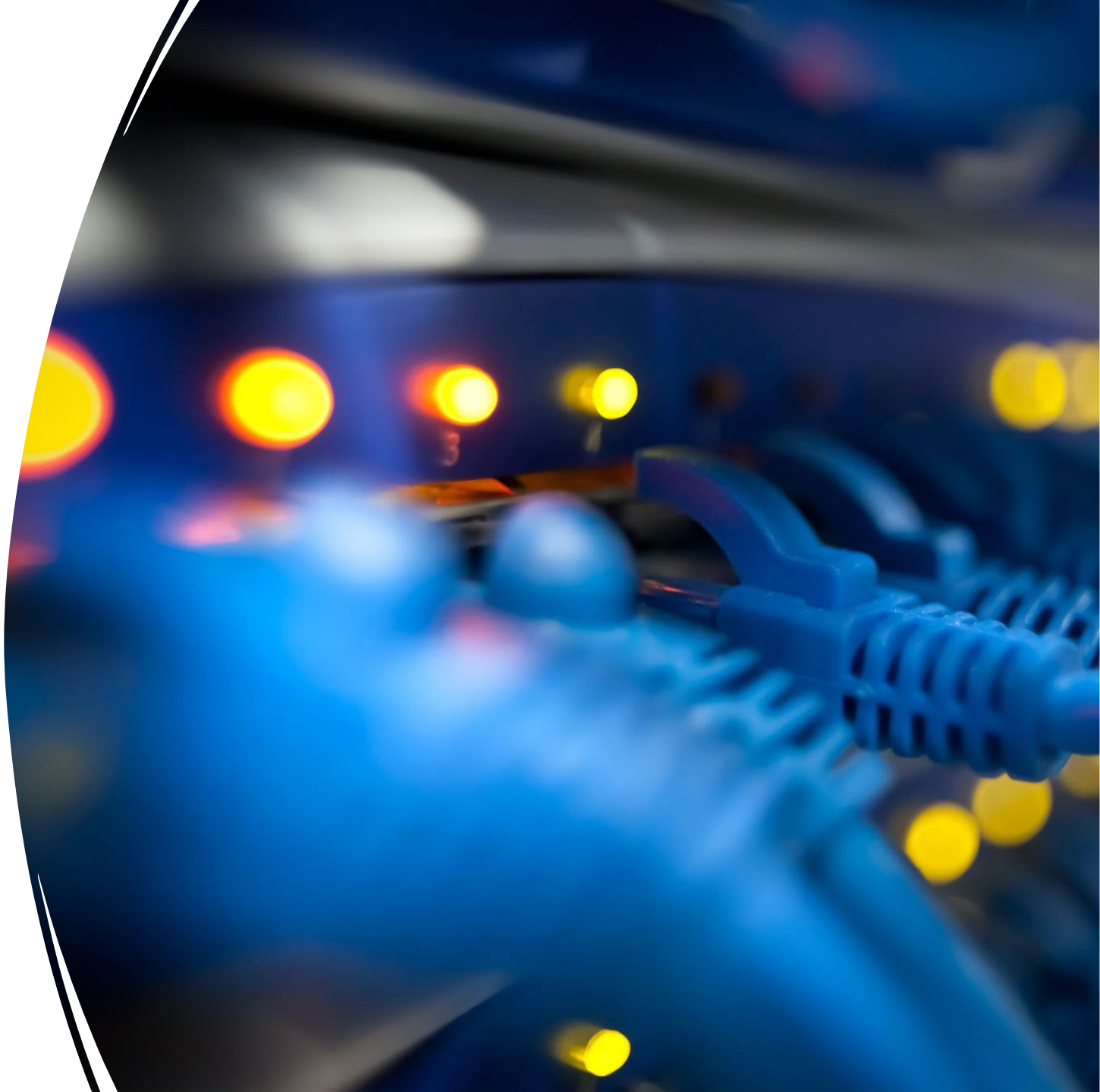
Quantum Networking

The first successful quantum key distribution (QKD) uplink from a fixed ground transmitter to a moving airborne receiver was demonstrated by a Canadian team from the University of Waterloo in 2017

This proof-of-principle experiment used a research aircraft to carry the receiver, successfully generating secure keys from a ground station while the aircraft flew at speeds up to 259 km/h and at altitudes around 1.6 km

Quantum Networking

March 2021, the Indian Space Research Organization (ISRO) successfully demonstrated free-space quantum communication over a 300-meter distance. This was the first time this type of communication was achieved in India and involved using quantum key distribution (QKD) to encrypt a live video conference. The demonstration took place at the Space Applications Centre (SAC) in Ahmedabad between two buildings within the campus



Quantum Networking

May 20, 2025, Quantum Key Distribution Networks Enhanced with Post-Quantum Onion Routing Security. https://quantumzeitgeist.com/quantum-key-distribution-networks-enhanced-with-post-quantum-onion-routing-security/

QKD Networks

Network	Location & scope	Key facts
Beijing–Shanghai trunk line (China)	China – backbone fiber between Beijing, Jinan, Hefei and Shanghai, ~2,000 km.	Opened in 2017; described as the first large-scale fiber QKD “trunk” line.
China integrated quantum communication network (China)	~4,600 km integrated network combining terrestrial fibre + satellites.	Described as the “world’s largest stable QKD network” in one report.
Madrid Quantum Communications Infrastructure (MadQCI) (Spain / Europe)	Metro-scale network in Madrid: “Europe’s largest and most complex quantum network” according to Toshiba.	Real-world telecom infrastructure, nine production sites, software-defined networking + QKD systems.
Nation-wide quantum safe key distribution network (South Korea)	South Korea – an ~800 km converged network connecting 48 government departments.	Described as “the world’s first country-wide quantum-safe network infrastructure”.

QKD Networks

Network (year)	Country/Region	Scale (approx.)	Notes / Status
Integrated space-to-ground QKD network (2021)	China	4,600 km end-to-end (2,000+ km terrestrial fiber + 2 satellite links)	Integrated 700+ fiber QKD links with satellite QKD; any user can reach any other via trusted nodes. Operational demo published in Nature.
Beijing–Shanghai "Jing-Hu" trunk line (2017)	China	~2,000 km fiber backbone	First national trunk QKD line; links Beijing–Jinan–Hefei–Shanghai; interfaced with the "Micius" QKD satellite. In service since Sep 29, 2017.
DemoQuanDT Berlin↔Bonn backbone (2024–25)	Germany	900+ km	DT fiber backbone demo with dynamic routing of QKD connections over long-haul.
National QKD network (SK Broadband/IDQ) (2022→)	South Korea	~800 km; 48 government departments	Country-wide "quantum-safe" infrastructure (QKD + classical integration). Reported as the largest outside China.
Chicago Quantum Network / IEQNET (2020–)	USA (Chicago metro)	124 miles (≈200 km); 6 nodes (2022)	Public testbed distributing quantum keys over city/suburbs; part of CQE; extends Argonne's 89-mile loop.
UKQN/UKQNtel (2019–)	United Kingdom	125 km (BT production fiber)	Real-world QKD over existing BT fiber with trusted nodes in BT exchanges; ongoing UK Quantum Communications Hub work.
MadQCI (Madrid QCI pilot) (2023–)	Spain / EU	Metro-scale; 9 production sites	Branded "Europe's largest and most complex" metro quantum network (vendor-agnostic SDN, multiple QKD systems).
Tokyo QKD Network (2010–)	Japan (Tokyo metro)	Multi-node testbed (≥6 links)	Long-running open testbed (NICT/JGN), trusted-node architecture; used for multi-vendor field trials.
SECOQC Vienna network (2008)	Austria (Vienna metro)	7 links, 5 sites	Early European multi-vendor QKD network across Siemens Austria subsidiaries; seminal architecture.
SwissQuantum (2009–2011)	Switzerland (Geneva metro)	Triangular 3-node network; 21-month run	Reliability/availability study in a live metro environment (Unige–CERN–hepia).
NQSN / NQSN+ (2022–)	Singapore	Nation-wide testbed (length not publicly specified)	Singapore-wide fiber access for quantum-safe pilots; now expanding with NQSN+ (hybrid QKD+PQC initiatives, incl. new carrier deployments).
OPENQKD testbeds (2019–)	Pan-EU (e.g., Berlin)	City testbeds up to ~100 km links	Multiple European pilots; Berlin star network on DT dark fiber; broader EU sites under OPENQKD.
DARPA Quantum Network (2003–2007)	USA (Boston/Cambridge)	10 nodes (metro)	World's first QKD network; mixed fiber/free-space; historic but foundational.
Abu Dhabi ADGM QKD testbed (2025–)	UAE (Abu Dhabi)	3-node metro pilot	First regional quantum-secure testbed in a live commercial (financial district) setting.
QUID – Quantum Italy Deployment (2023–)	Italy (national)	Multi-city QMANs + national backbone (in progress)	EuroQCI national rollout linking 7+ cities and long-haul corridors (e.g., Bologna–Trieste).

NSA Limits of QKD

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.
6. -https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

The NSA on QKD and Quantum Cryptography

- **What are Quantum Key Distribution (QKD) and Quantum Cryptography (QC)?**
- Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link. Published theories suggest that physics allows QKD or QC to detect the presence of an eavesdropper, a feature not provided in standard cryptography.
- Quantum-resistant algorithms are implemented on existing platforms and derive their security through mathematical complexity. These algorithms used in cryptographic protocols provide the means for assuring the confidentiality, integrity, and authentication of a transmission—even against a potential future quantum computer. The National Institute of Standards and Technology (NIST) is presently conducting a rigorous selection process to identify quantum-resistant (or post-quantum) algorithms for standardization[1]. Once NIST completes its selection process, NSA will issue updated guidance through CNSSP-15.

Comparison of Protocols

Protocol Name	Authors; year; reference	Type	Principles	PNS safe	Efficiency	Specialty
BB84	C. H. Bennett and G. Brassard; 1984 [11]	DV	Uncertainty	No	~N/4	First in the history QKD.
E91	A. Ekert; 1991 [12]	DV	Entanglement	Yes	~N/2	First in the history EPR-based QKD.
BBM92	C. H. Bennett, G.Brassard and N. D. Mermin; 1992 [13]	DV	Uncertainty	No	~N/3	First experimental QKD. Introduced parity check and hashing methods during information reconciliation.
BB92	C. H. Bennett; 1992 [14]	DV	Uncertainty	No	~N/2	Uses two non-orthogonal low-intensity coherent states.
MSZ96	Yi Mu, Jennifer Seberry, Yuliang Zheng; 1996 [22]	CV	Uncertainty	N/A	~N/2	No units polarized photons, bit encoded in four non-orthogonal states described by quadrature phase amplitudes of a weak optical field.
DI	D.Mayers and A.Yao; 1998 [25]	DV	Uncertainty	N/A	Extremely low [26]	First device independent QKD.
SSP	H. Bechmann-Pasquinucci and N. Gisin; 1999 [16]	DV	Uncertainty	No	~N/3	The symmetry of this protocol simplifies considerably the security analysis.
DPS	K.Inoue, E.Waks and Y.Yamanoto; 2003 [15]	DV	Uncertainty	Yes	~N [15]	Utilises all photons for creating the key, simple configuration, efficient time domain use.
BB84 decoy state	W.-Y. Hwang; 2003 [17]	DV	Uncertainty	Yes	~N/2	First proposed a decoy-state method to overcome the PNS attack in the presence of high loss.
SARG04	V. Scarani, A. Acin, G.Ribordy and N. Gisin; 2004 [18]	DV	Uncertainty	No [28]	~N/6	Encoding classical bit in sets of non-orthogonal states, made significant robust against PNS attack.
COW	N.Gisin, G. Ribordy, H.Zbinden, D. Stucki, N. Brunner, V.Scarani; 2004 [24]	CV	Uncertainty	Yes	~N, decreases linearly	The information is encoded in time. Additional communication line allows monitoring the presence of a spy.
KMB09	M. M. Khan, M. Murphy, and A. Beige; 2009 [19]	DV	Uncertainty	Yes	~N/4	Two mutually unbiased bases used. Index transmission error rate was introduced.
S09	E. H. Serna; 2012 [27]	DV	Uncertainty	N/A	~N	Public crypto QKD. Can be implemented for more than two parties. One-photon protocol version persists.
MDI	H.-K. Lo, M. Curty and B. Qi; 2012 [26]	DV	Uncertainty	Yes	~N/6	Works even when Alice and Bob's preparation processes are imperfect.
S13	E. H. Serna; 2013 [28]	DV	Uncertainty	N/A	~N, ~4N [28]	Public crypto QKD. Generates various secret keys of the transmitted qubits, implying zero information losses between the interlocutors.
T12	Toshiba Research Europe; 2013 [21]	DV	Uncertainty	Yes	~N	Rectilinear (+) is the majority basis. Three intensity values are used. Equipment controls QBER continuously.
AE17	A. A. Abushgra and K. M. Elleithy; 2017 [22]	DV	Uncertainty, Entanglement	Yes	~N	Designed matrix that includes decoy states and parity check. EPR authentication phase, where EPR string is used as a key for the whole system.

Conclusions

- Questions??