

# US Stock Express

Daniel Yue

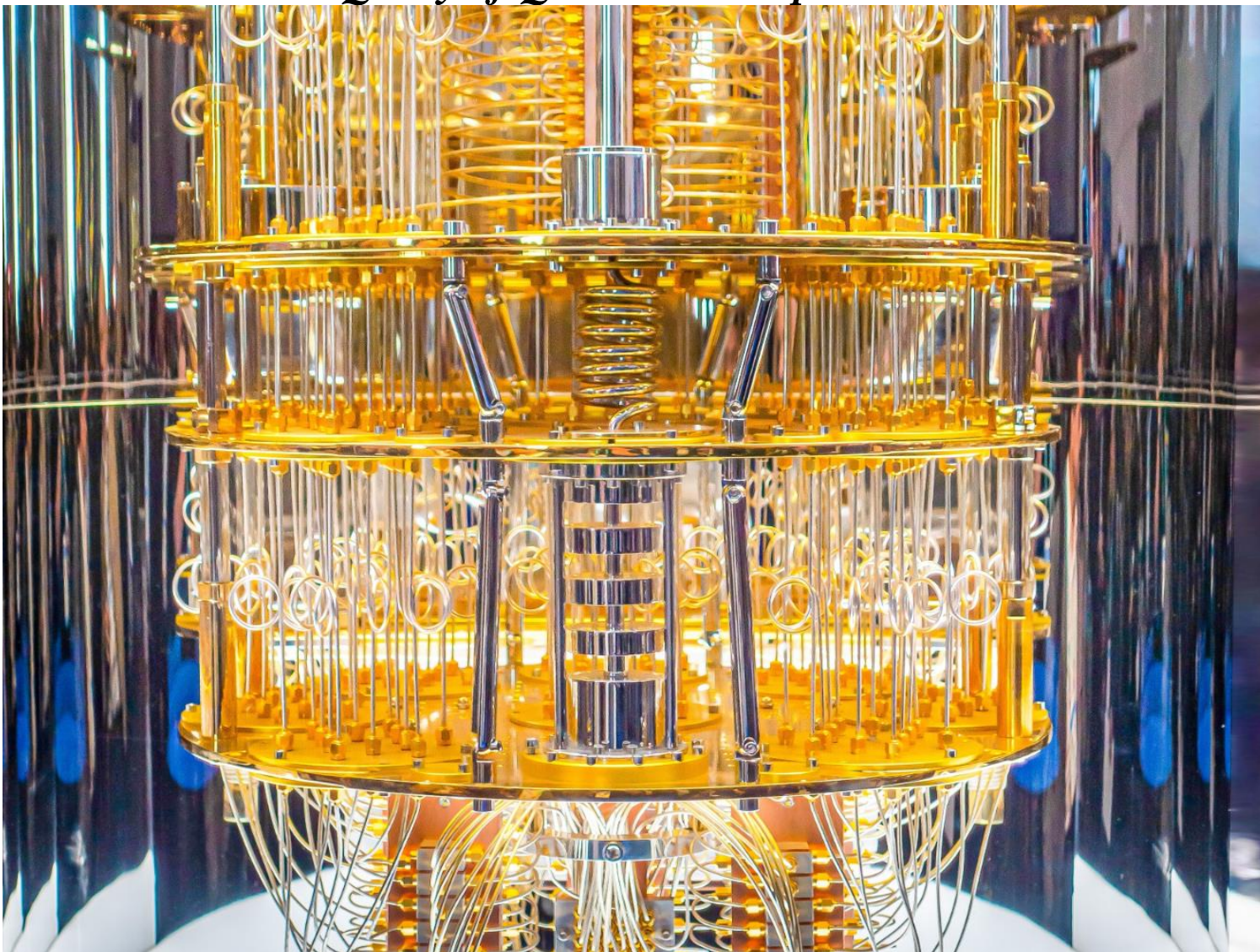
Email: [info@ihandbook.org](mailto:info@ihandbook.org)

[www.ihandbook.org](http://www.ihandbook.org)

©



## *Q Day of Quantum Computer*



*Q-Day refers to the hypothetical day when quantum computers become powerful enough to break current encryption methods, posing significant risks to cybersecurity. (Copilot)*

# *Each dot at the back of Milky Way is a Galaxy*

## Financial Astrology & Chinese Geomancy

Online Training Course

The first patch aims at improving your personal luck

### START DATE

April 26, 2026 (Sun)

### ENROLMENT

[ihandbook.org](http://ihandbook.org) → contact form

### FORMAT

12 lectures  
(6 by email,  
6 online discussions)

### FEE

US\$275

### MENTOR

Daniel Yue

[iHandbook.org](http://iHandbook.org)

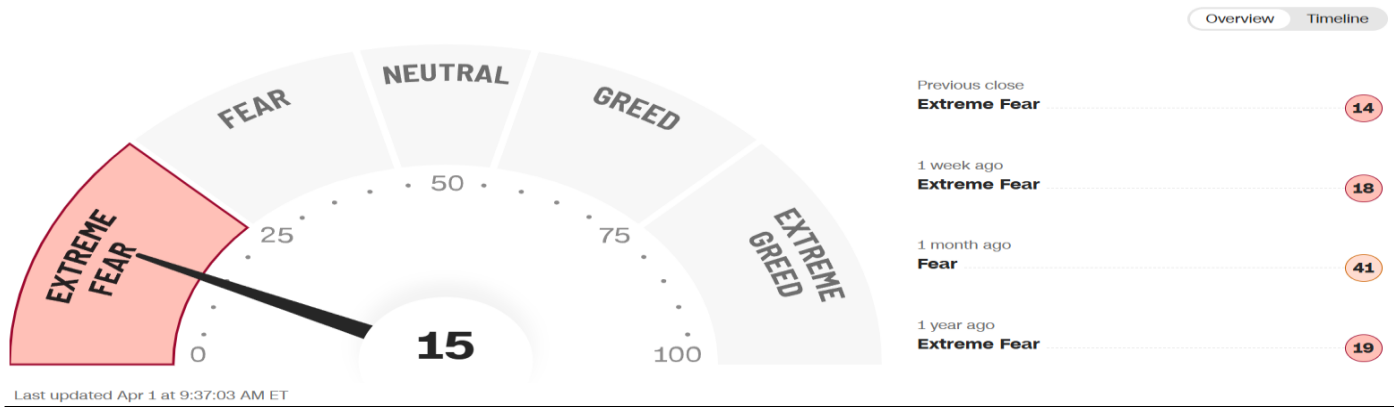
When Donald Trump gave his 48-hour ultimatum on Friday, Elon Musk announced his project of “Terafab” on Saturday, saying the universe is so enormous, the sun occupies 98% of mass in solar system, why we are having so much disputes on earth. He is developing the largest solar energy project, let’s response with improving your personal luck by solar calendar of Geomancy in our training course, rather than aiming at meaningless human disputes on this or that location on earth. The earth is just a tiny dot in solar system. The solar system is just a tiny dot in Milky Way. The Milky Way is just a tiny dot ..... So, forget all those disputes and improve your own luck first.

YouTube Video : [102\) 4 great channel crises leading to World War 3. Auspicious time of buying lottery by Astrology.](#)

*Risk disclosure: Price can go up and down at any moment, use free money to trade and bear the risk according to your own capital;  
 Never trade with money that has a deadline for withdrawal.  
 All suggestions are for reference only, even AI cannot be 100% reliable, final decision still lies upon investors.  
 Copy trading cannot replicate another trader's background or psychological state.*

# Fear & Greed Index

What emotion is driving the market now?  
[Learn more about the index](#)



**Holiday Notice:**  
 April 3 is Good Friday which is market holiday. The Express will clock off on that day. We apologize for any inconvenience caused. Since the writer will be away from Hong Kong, *from April 6 (Mon) to April 8 (Wed), Professor Vitaliy will handle the comments* and Daniel Yue will be back to post on April 9 (Thu).





World Observation

Day 1499  
Russia/Ukraine Conflict

## Stocks for Tomorrow

The war in Iran surely will have an end one day, what investors need to do now is to aim at stocks of tomorrow rather than who is right or who is wrong, who has got pyrrhic victory and who can maintain their own face. Anyway, the United Nations is the loser, for the nuclear talk started in 2006 of P5+1 and after 20 years this is the result. They took no part in the war or peace and even no one asked them to be a middleman.

Investors at once go back to the situation of last year, that is too many potential stocks need to buy, but too little capital in hand. What should do is to forget the past and look forward. Of course, one of the hottest topics of the market is the Artemis Project. Most of the stocks of the space industry are duplicated with military stocks, investors can refer to The Express of 20260326.

Retail investors better target their focus to Q-Day of quantum computers.

Another new page has already turned on. Do not stick to whatsoever AI, robots performing Kung Fu fighting, Full Self Driving taxi in San Francisco or smuggling of chips to here and there, or keep on arguing is the current AI trend a bubble.

No ! No ! No !

However, another hot topic nowadays beyond the Middle East is Q-Day of quantum computers. It will replace petroleum, aircraft carrier strike group,

Bunker Buster Bomb, enriched uranium, B2 bombers and F35 fighters. Q-Day is the term used to describe the moment when a quantum computer can effectively break widely used encryption algorithms ..... where the security of sensitive data, including emails, bank transactions, and government secrets will be compromised easily. Another new era of quantum is arriving. At first said to be in 2048-2050, later said 2030-2031, now confirmed the Q-Day is as early as 2029.

It does not mean the quantum computer will replace the traditional computer. That is no matter in the office or at home, traditional computers are still used as nowadays. Traditional computers use the 0 and 1 bits. That is when you type the word *boy*, there is no such word stored inside the computer for you to call it out. The computer at first ask is it “a”, when no the signal is 0, then carry on the next one to ask is it “b”, when it is the signal is “1”, and then carry on the next letter “o”, but have to start from again with “a”, anyway to ask one by one with 0 and 1. But quantum computers start with billions of times billions of signals to ask all at once, that is why they can decipher all codes.

So, in the financial market, not only can it intrude on all secret documents, but also can decipher the golden key for crypto. That means all codes are no longer confidential in front of quantum computers, what they need to do is another anti-quantum computer format.

What stocks we need to buy? Please refer to the commendations and explanations of AI one by one. Take action before it is too late. A smart investor should run ahead of the era, and do not be a follower. One should know the trend faster than others. Do not just do copy trade, no use to copy from Warren Buffet or Cathy Wood, for their background is too far away from us. Even the AI gave a lot of recommendations, they always say *better do the research on your own*.

**Quantum computers differ fundamentally from traditional ones by using qubits that can exist in multiple states simultaneously, enabling exponential speedups in certain tasks. If “Q-Day” arrives earlier than expected (2029–2031), it could break current cryptographic systems, including Bitcoin’s elliptic curve signatures, but post-quantum cryptography is already being developed to defend against this. NVIDIA is not building quantum computers directly; instead, it focuses on GPU-based acceleration and interconnects like NVLink/NVQLink to support hybrid quantum-classical systems. For retail investors, diversified ETFs and tech enablers (like NVDA) remain safer bets than speculative quantum startups.**

### ◆ Traditional vs Quantum Computers

- **Traditional computers:** Use *bits* (0 or 1), governed by classical physics. They process instructions sequentially.
- **Quantum computers:** Use *qubits*, which leverage **superposition** (0 and 1 simultaneously) and **entanglement**. This allows massive parallelism and faster solutions for problems like factoring large numbers or simulating molecules.

GeeksForGeeks + 1



GPT-5 is here - OpenAI

Passed Turing Test as AGI (super AI) level

### ◆ Q-Day & Financial Market Impact

- **Q-Day:** The moment when quantum computers can break widely used cryptographic systems.
- **Bitcoin risk:** Elliptic curve cryptography (ECC) could be broken, allowing forged signatures and stolen coins. Early wallets with exposed public keys are most vulnerable. Decrypt + 1
- **Financial markets:** If cryptography across banks, trading systems, and blockchains is compromised, confidence could collapse. Expect volatility, regulatory intervention, and rapid migration to quantum-safe systems. Forbes

### ◆ Anti-Quantum Cryptography

- **Post-quantum cryptography (PQC):** Algorithms designed to resist quantum attacks, based on lattice problems and hash functions.
- **NIST standards:** Four quantum-resistant algorithms have already been selected and standardized. Wikipedia + 2
- **Outlook:** Migration to PQC is underway, so financial systems and Bitcoin can adapt before Q-Day.

◆ **NVIDIA's Role & NVLink**

- **Why NVIDIA doesn't build quantum computers:**
  - Quantum hardware is highly specialized (superconducting qubits, trapped ions).
  - NVIDIA's strength lies in GPUs, AI, and simulation. It enables quantum research rather than competing with IBM/Google. [The Quantum Insider + 1](#)
- **NVLink:** A high-speed GPU interconnect providing **5x PCIe bandwidth**, enabling GPUs to share memory directly. [Wikipedia + 1](#)
- **NVQLink:** Extends NVLink to connect GPUs with quantum processors, supporting hybrid quantum-classical computing. [Nvidia](#)
- **Comparison with quantum computers:** NVLink is classical infrastructure; quantum computers are fundamentally different. NVLink accelerates AI/HPC today, while quantum computing is still experimental.

◆ **Retail Investor Strategy**


- **Diversification is key:**
  - **Tech enablers:** NVIDIA (NVDA), AMD, and cloud providers (MSFT, GOOG) benefit from AI + quantum integration.
  - **Quantum-safe cybersecurity firms:** Companies working on PQC standards.
  - **ETFs:** Safer exposure, e.g., RBC Target 2026 Canadian Corporate Bond Index ETF (RQO), yielding ~2.75% with low risk. [MSN 財經](#)

**RBC Target 2026 Canadian Corporate Bond Index ETF (RQO)**

31 Mar, 3:54 pm EDT • Market closed

**18.85** CAD

-0.01 (-0.05%) Today

 **GPT-5 is here - OpenAI**  
*Passed Turing Test as AGI (super AI) level*

 **Quick Comparison**

| Aspect              | Traditional Computer | Quantum Computer                | NVIDIA NVLink/ NVQLink            |
|---------------------|----------------------|---------------------------------|-----------------------------------|
| Core unit           | Bit (0 or 1)         | Qubit (0, 1, both)              | GPU interconnect                  |
| Speedup potential   | Linear scaling       | Exponential in certain problems | 5x PCIe bandwidth                 |
| Cryptography impact | Secure today         | Can break ECC/RSA               | Supports AI/HPC, not cryptography |
| NVIDIA's role       | Dominant GPU maker   | Partner ecosystem               | Infrastructure enabler            |

✓ **Bottom line:** Quantum computing will disrupt cryptography, but PQC standards are already in place to defend against it. NVIDIA is positioning itself as the infrastructure backbone rather than a quantum hardware builder. For retail investors, balanced exposure to tech enablers (NVDA, MSFT, GOOG) and safe ETFs is a prudent strategy.

Would you like me to build a **scenario matrix of Q-Day impacts on Bitcoin vs traditional finance** so you can visualize risk/reward timelines? [GeeksForGeeks + 1](#) [Decrypt + 1](#)

[Forbes](#) [Wikipedia + 2](#) [The Quantum Insider + 1](#) [Wikipedia + 1](#) [Nvidia](#) [MSN 財經](#)

**Google's recent update on Q-Day (the point when quantum computers could break today's public-key encryption like RSA and ECC) is accurate.** In late March 2026, Google publicly shortened its internal migration timeline for post-quantum cryptography (PQC) to 2029. This shift was driven by faster-than-expected advances in quantum hardware, error correction, and revised resource estimates for running algorithms like Shor's (e.g., breaking 256-bit elliptic curve discrete logarithm problems with roughly 20x fewer physical qubits than previously modeled—under 500,000 physical qubits on a superconducting system for ECDLP-256 in minutes). Previously, many timelines (including Google's alignment with broader industry/government targets) pointed to 2030–2035 or later, with original long-term projections in the 2040s. Google is now urging the industry (banks, governments, tech providers, and crypto) to accelerate PQC adoption. [Blog +2](#)

## Difference Between Traditional (Classical) Computers and Quantum Computers

Traditional computers (what we use every day—phones, laptops, servers) rely on **bits** that are strictly 0 or 1. They process information sequentially or in parallel using transistors, logic gates, and deterministic algorithms. This works great for most tasks (word processing, web browsing, basic AI training) but struggles with certain "hard" problems that require checking an enormous number of possibilities (e.g., factoring huge numbers or searching unsorted databases).

Quantum computers use **qubits**, which can exist in a superposition of 0 and 1 at the same time (thanks to quantum mechanics). They also leverage **entanglement** (linking qubits so the state of one instantly influences another, regardless of distance) and **interference** (to amplify correct answers and cancel wrong ones). This enables massive parallelism: a system with  $n$  qubits can represent  $2^n$  states simultaneously.

The result is exponential speedup for specific problems:

- Shor's algorithm (quantum) can factor large numbers or solve discrete logarithms in polynomial time → breaks RSA/ECC encryption.
- Grover's algorithm speeds up unstructured search.
- Quantum simulation excels at modeling molecules/chemistry.

Classical computers remain superior (and far more practical/cheap/scalable) for everyday tasks.

Quantum computers are not "faster general-purpose machines"—they are specialized accelerators that require extreme conditions (near-absolute zero temperatures for most types) and heavy classical support for error correction and control. Current quantum machines are noisy intermediate-scale (NISQ) with dozens to hundreds of qubits; a "cryptographically relevant" one (CRQC) needs fault-tolerant logical qubits in the thousands to millions. [Research](#)

## Will Q-Day Decipher Codes in Financial Markets (Including Bitcoin Keys)? What Is the Impact?

**Yes, a CRQC by ~2029 could break most current public-key cryptography.** This includes:

- RSA and ECC used in TLS/SSL (secure web browsing, banking apps, VPNs).
- Digital signatures for authentication and non-repudiation.
- Many blockchain systems, including Bitcoin's ECDSA (Elliptic Curve Digital Signature Algorithm) for transaction signing and wallet security.

For Bitcoin specifically: Google's latest research shows the resource requirements for breaking ECDLP-256 dropped dramatically. An attacker with a CRQC could derive private keys from public keys (exposed in many transactions or reused addresses). "Store-now-decrypt-later" (SNDL) attacks are already a real risk—adversaries could harvest encrypted financial data today and decrypt it later. [Research +1](#)

**Financial market impacts** would be severe if migration lags:

- Widespread breaches of encrypted communications, certificates, and signatures.
- Forged transactions or stolen funds in banking, trading platforms, and DeFi.
- Loss of trust → market volatility, bank runs, or crypto flash crashes.
- Systemic risk in payment systems, derivatives clearing, and custody.

However, this is not an overnight "all codes broken tomorrow." Full-scale CRQCs won't appear instantly, and "harvest now" only affects data stored unprotected. The bigger near-term issue is digital signatures (future threat) versus confidentiality (present risk). The financial sector (and crypto projects like Ethereum Foundation, Coinbase) is already collaborating on PQC transitions.

## Anti-Quantum Cipher Codes to Fight It?

**Yes—post-quantum cryptography (PQC) already exists and is being standardized/rolled out.** These algorithms are designed to resist quantum attacks (based on problems like lattices, hashes, or codes that Shor's algorithm doesn't break efficiently). Key examples:

- NIST standards (finalized in recent years): ML-KEM (Kyber) for key encapsulation, ML-DSA (Dilithium) and SLH-DSA for signatures.
- Google is integrating these into Android, Chrome, and its infrastructure, targeting full migration by 2029.
- Bitcoin and other blockchains can (and plan to) upgrade via hard forks to quantum-resistant signatures.

Migration is the defense: "hybrid" schemes (classical + PQC) are already in use for backward compatibility. Governments (U.S. via NIST/NSA timelines) and industry are pushing hard. The clock is ticking, but the tools exist. [Blog](#)



## Why Doesn't NVDA (Nvidia) Develop Quantum Computers?

Nvidia's strategy is deliberate: **they are not trying to build qubits or quantum processors themselves.** Quantum hardware is physics-intensive (superconducting circuits, trapped ions, photons, etc.) with huge engineering challenges around error rates, cooling, and scalability. Nvidia instead leverages its dominance in classical accelerated computing (GPUs, CUDA) to *enable* and *accelerate* quantum progress:

- They provide GPU-based simulation, optimization, and error-correction tools (CUDA-Q platform).
- Their tech helps researchers design better qubits, compile circuits faster, and run hybrid quantum-classical workloads.
- This maximizes leverage from their existing ecosystem rather than entering a capital-intensive, high-risk hardware race.

Nvidia views quantum as needing massive classical support anyway—GPUs handle the heavy lifting for control, calibration, and error decoding. [Thequantuminsider +1](#)

## What Is NVA-Link (NVLink)? How Does It Compare to a Quantum Computer?

It's almost certainly **NVLink** (Nvidia's proprietary high-speed interconnect for classical GPUs/CPUs). NVLink enables direct, ultra-low-latency, high-bandwidth communication between multiple GPUs (up to terabytes per second in modern generations) in AI/HPC clusters—far faster than PCIe. This powers massive parallel classical computing for training giant AI models.

Nvidia has also introduced NVQLink (2025), an open architecture that extends this idea to **hybrid quantum-classical systems**: it tightly couples quantum processing units (QPUs) with GPU supercomputers for real-time tasks like quantum error correction, calibration, and hybrid apps. [Nvidia +1](#)

**Comparison to a quantum computer:** NVLink/NVQLink is *not* quantum computing—it is classical infrastructure. It scales and supports quantum hardware (making QPUs usable at scale) but doesn't perform quantum operations itself. A true quantum computer relies on qubits and quantum effects for exponential advantage on specific problems; NVLink is about connecting classical GPUs efficiently. Think of it as the "highway system" that helps quantum cars reach their destination faster.

## Stocks Retail Investors Can Buy (in the Context of Quantum Advancement/Q-Day)

Quantum computing is still early-stage and volatile—pure-play stocks can swing wildly on news. This is **not financial advice**; do your own research, consider diversification, and note high risk (many are pre-revenue or speculative). Publicly traded options include:

**Pure-play quantum hardware/software companies** (direct exposure to building quantum tech):

- **IONQ** (NYSE: IONQ) — Trapped-ion quantum computers; one of the most prominent pure plays.
- **RGTI** (NASDAQ: RGTI) — Rigetti Computing; superconducting qubits and full-stack quantum.
- **QBTS** (NYSE: QBTS) — D-Wave Quantum; quantum annealing (specialized for optimization problems).
- **QUBT** (NASDAQ: QUBT) — Quantum Computing Inc.; focuses on quantum hardware, software, and photonics.

**Established/big-tech players with major quantum programs** (more stable, diversified exposure):

- **IBM** (NYSE: IBM) — Long-time quantum leader with cloud access and hardware roadmap.
- **NVDA** (NASDAQ: NVDA) — Indirect play via its enabling role (CUDA-Q, NVQLink, hybrid acceleration); benefits from quantum R&D demand without building QPUs.
- Others like **MSFT**, **GOOG/GOOGL** (Alphabet/Google), **AMZN**, or **HON** (Honeywell/Quantinuum) also invest heavily but quantum is a small part of their business.

There are also smaller PQC-focused firms (e.g., SEALSQ, BTQ) and ETFs like Defiance Quantum ETF for broader exposure. The Q-Day urgency is accelerating investment in both quantum hardware *and* quantum-resistant security—favoring companies actively migrating or enabling the transition.

Thequantuminsider +1

In summary, Q-Day is moving closer (2029 per Google), creating both risks (encryption breakage) and opportunities (PQC upgrades, quantum tech acceleration). Classical computing giants like Nvidia are positioning to support the hybrid future rather than compete directly in qubits. Stay informed—the transition is happening now.