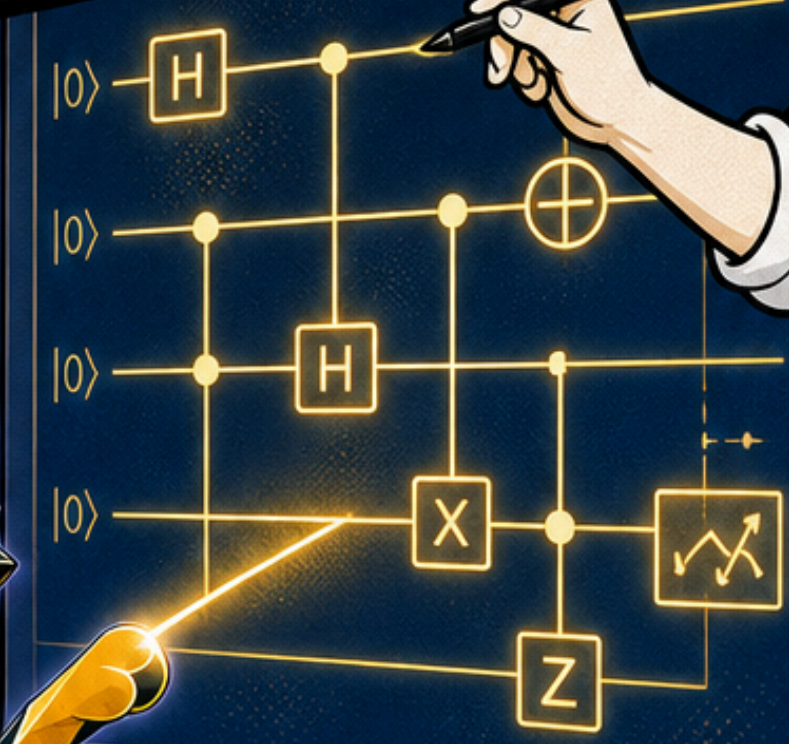


QUANTUM COMPUTING EXPLAINED: WHAT IT ACTUALLY DOES AND WHY IT MATTERS



THE CLASSICAL BIT: SMALL, RELIABLE, STUBBORN

Every device you've ever used to compute something, from a smartphone to the world's fastest supercomputer, works with bits. A bit is binary: it's either a 0 or a 1. That's it. The entire internet, every app, every spreadsheet, every AI model runs on enormous cascades of those two states switching very, very fast.

Bits are brilliant at what they do. Put one in a state and it stays there, which is exactly what you want from stable, reliable computation. But that stability is also a constraint. A classical computer can only be in one state at a time. To solve a complex problem with many possible answers, it has to check options one by one, or in managed parallel batches, working through the solution space methodically.

For most problems, that's fine. For some problems, it's impossibly slow.



QUBITS: THE SWITCH THAT ISN'T



A quantum computer replaces bits with qubits. The difference isn't just a new name. It's a fundamentally different physical behaviour.



A classical bit is like a light switch: it's either on or off.



A qubit is sometimes compared to a spinning coin that appears to be simultaneously heads and tails until it lands — but that analogy has an important limit.

A spinning coin has a definite face we simply haven't observed yet; a qubit in superposition genuinely has no definite value until the act of measurement itself determines the outcome.

This property is called **superposition**, and it means a qubit can exist as 0, as 1, or as a combination of both at the same time.

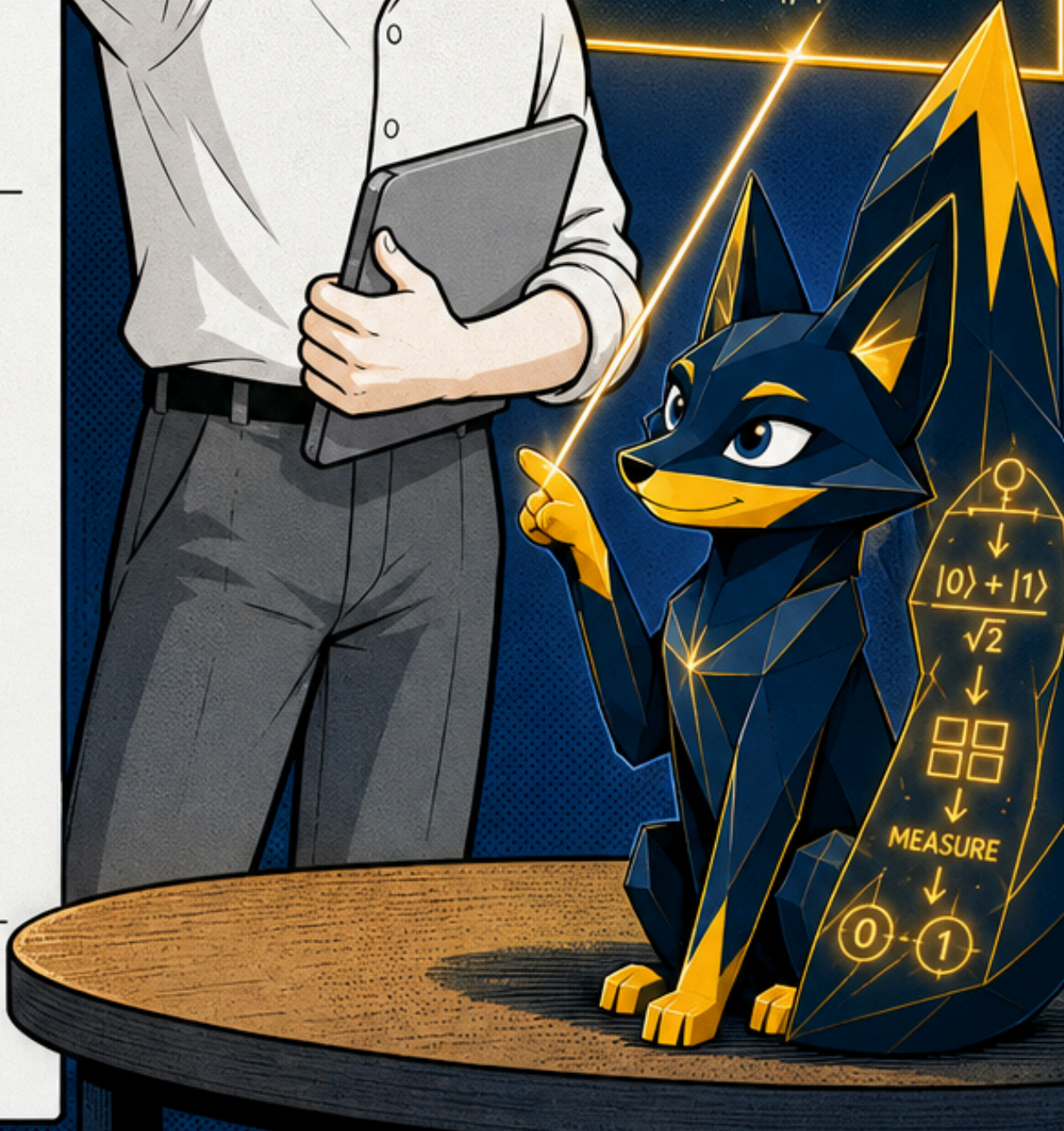
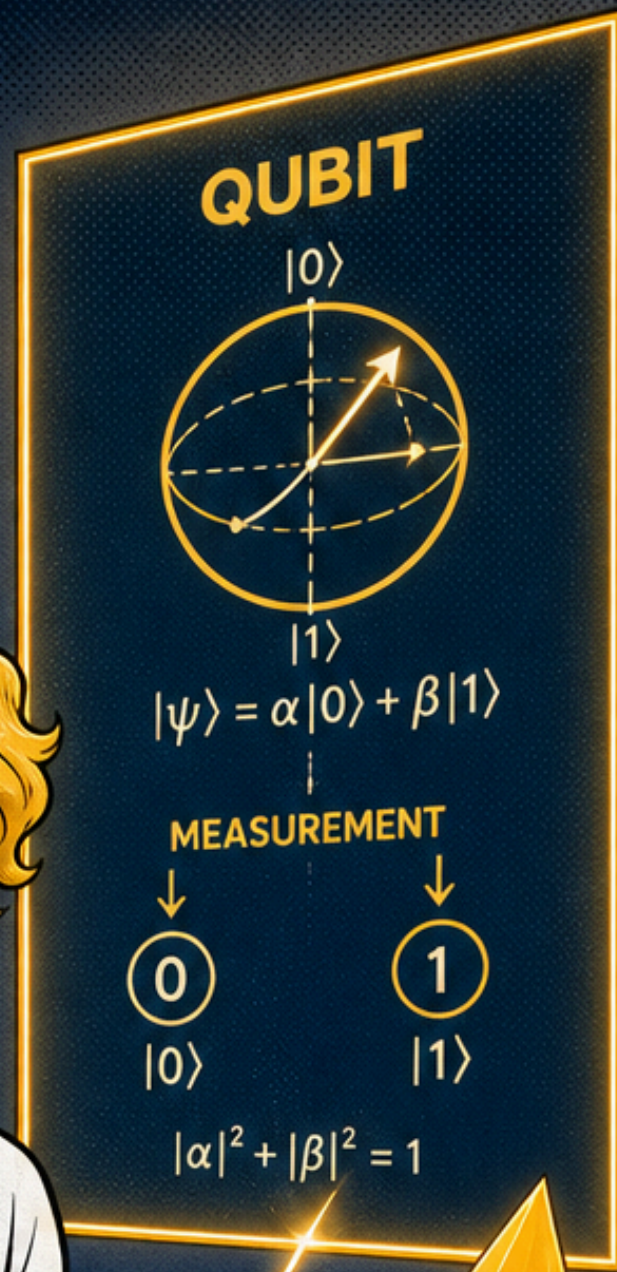
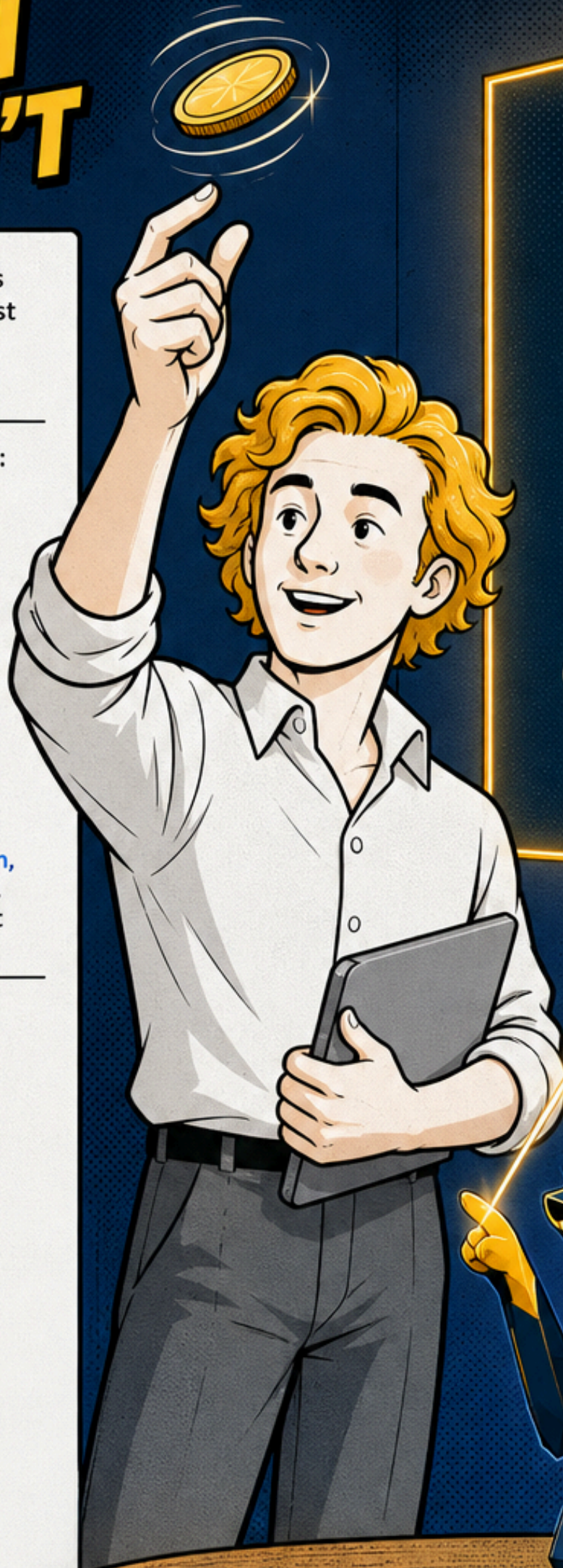


That might sound like a curiosity, but the practical consequence scales fast.

- With **2** qubits, **4** states.
- With **3** qubits, **8** states.
- With every additional qubit, the number of simultaneously represented states doubles.
- By **20** qubits, a quantum processor can operate across **more than a million** states at once.
- By **300** qubits, the number of representable states mathematically **exceeds the estimated number of atoms in the observable universe**—though it's worth noting that representing those states is not the same as usefully accessing all of them for arbitrary problems. The practical power depends heavily on the algorithm and problem structure.



This isn't magic. It's quantum physics applied to computation, and it gives quantum machines a **very specific kind of power for a very specific kind of problem.**



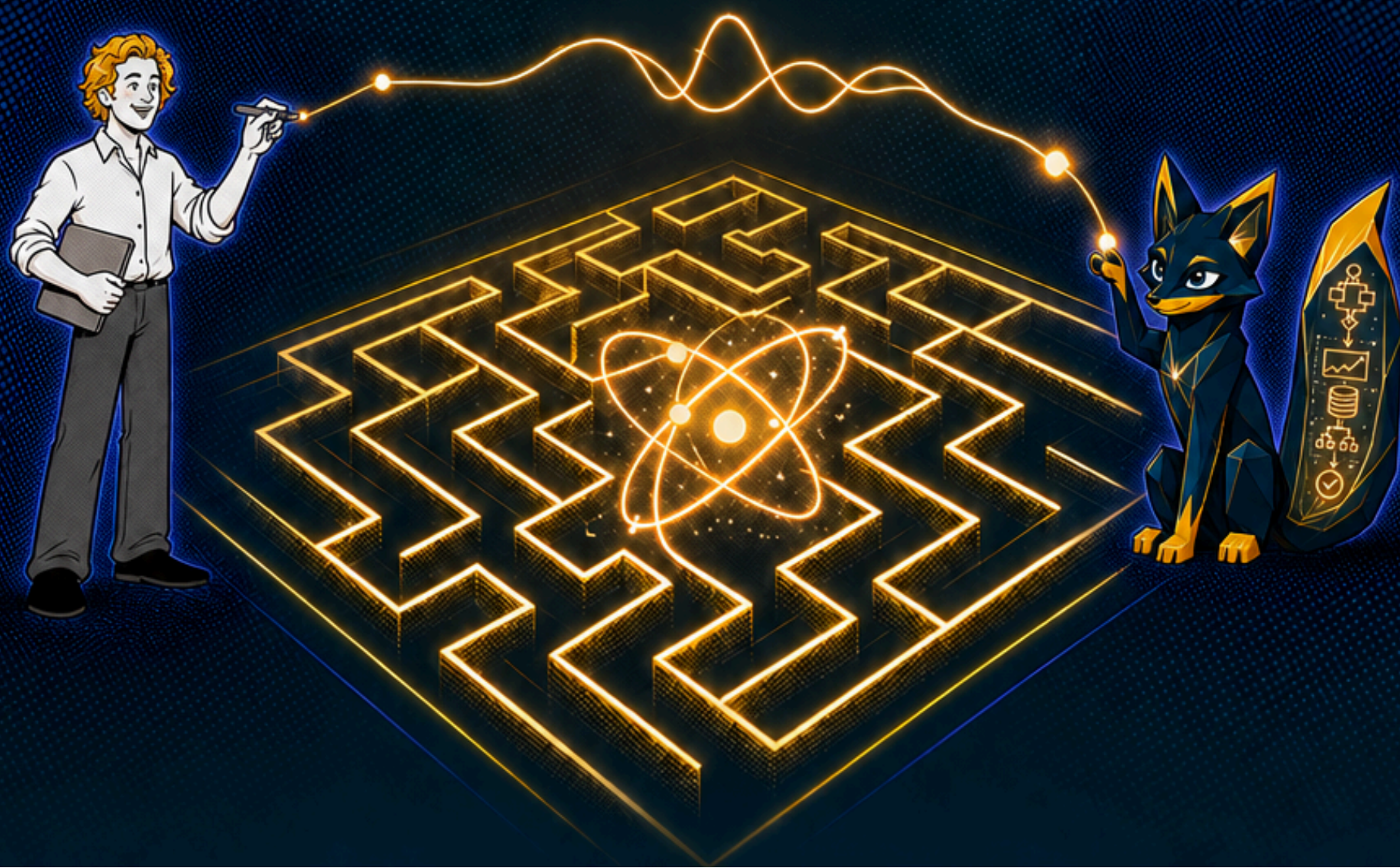
ENTANGLEMENT: QUBITS THAT THINK TOGETHER

Superposition alone doesn't fully explain quantum computing's power. The second piece is **entanglement**: the ability of two or more qubits to become linked so that the state of one instantly influences the state of the others, regardless of the distance between them.

When qubits are entangled, they stop behaving as independent units. **Measure one, and you immediately know something about all the others.**

This allows quantum computers to coordinate information across qubits in ways classical computers simply can't replicate, enabling **genuinely parallel computation** where the machine isn't just checking options in sequence but exploring many solutions simultaneously as a connected system.

Think of it this way: a classical computer solving a maze tries one path at a time. **An entangled quantum system explores branches of the maze as a coordinated whole**, not one-by-one.



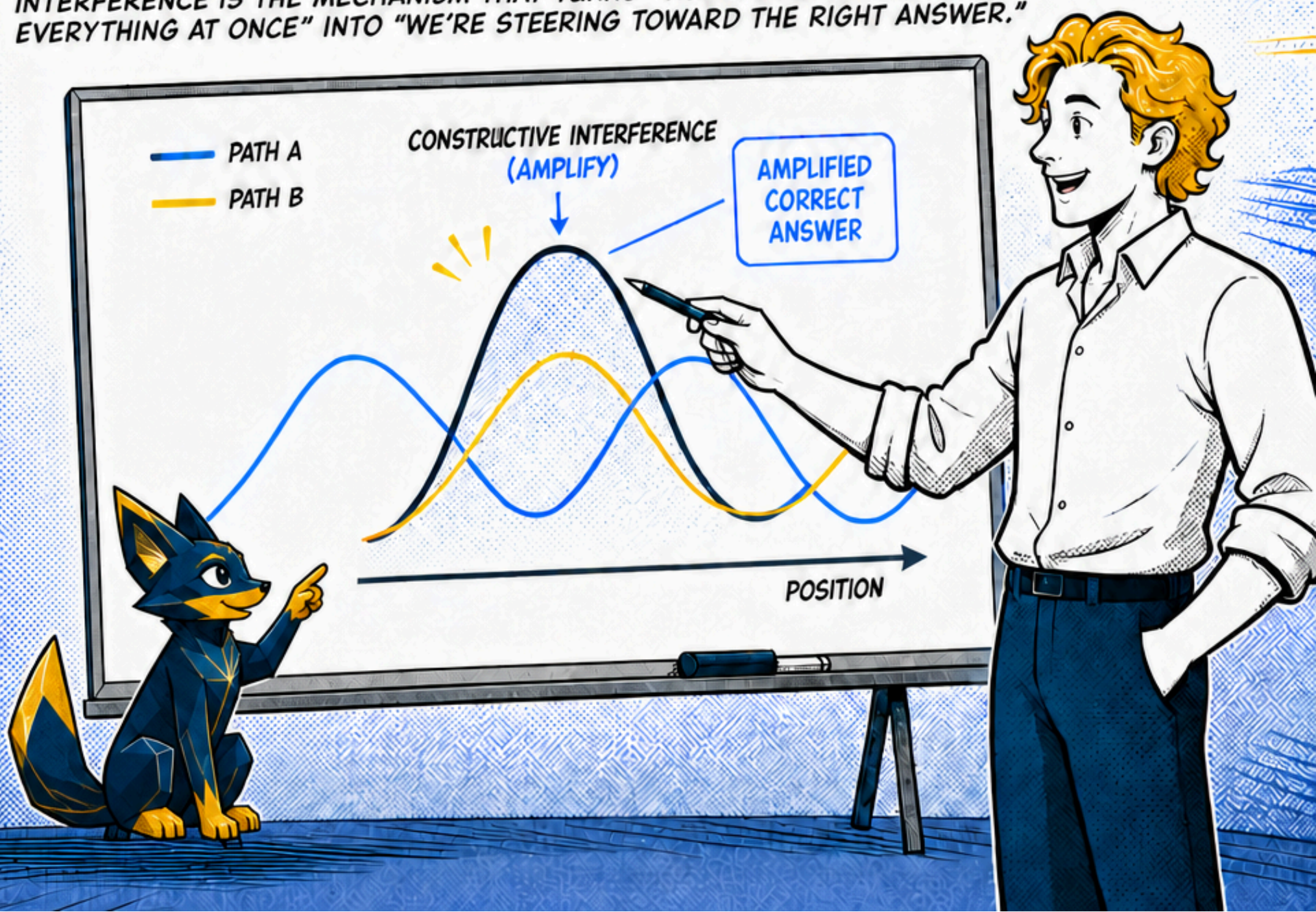
INTERFERENCE:

FILTERING TOWARD THE RIGHT ANSWER


SUPERPOSITION AND ENTANGLEMENT GIVE A QUANTUM COMPUTER A VAST SOLUTION SPACE TO EXPLORE. BUT EXPLORING EVERY POSSIBILITY SIMULTANEOUSLY WOULD JUST PRODUCE A USELESS BLUR OF OUTCOMES WHEN THE MACHINE IS MEASURED. THIS IS WHERE THE THIRD PRINCIPLE, **QUANTUM INTERFERENCE**, DOES THE CRITICAL WORK.


QUANTUM STATES BEHAVE LIKE WAVES. AND JUST AS TWO WAVES CAN AMPLIFY EACH OTHER OR CANCEL EACH OTHER OUT WHEN THEY OVERLAP, QUANTUM ALGORITHMS ARE DESIGNED SO THAT CORRECT COMPUTATIONAL PATHS **CONSTRUCTIVELY INTERFERE** AND BECOME MORE PROBABLE, WHILE INCORRECT PATHS **DESTRUCTIVELY INTERFERE** AND BECOME LESS PROBABLE.


THE RESULT: WHEN THE QUANTUM SYSTEM IS FINALLY MEASURED AND ITS SUPERPOSITION COLLAPSES TO A DEFINITE ANSWER, THE PROBABILITY OF LANDING ON THE CORRECT ANSWER HAS BEEN **DELIBERATELY AMPLIFIED**. INTERFERENCE IS THE MECHANISM THAT TURNS "WE'RE LOOKING AT EVERYTHING AT ONCE" INTO "WE'RE STEERING TOWARD THE RIGHT ANSWER."



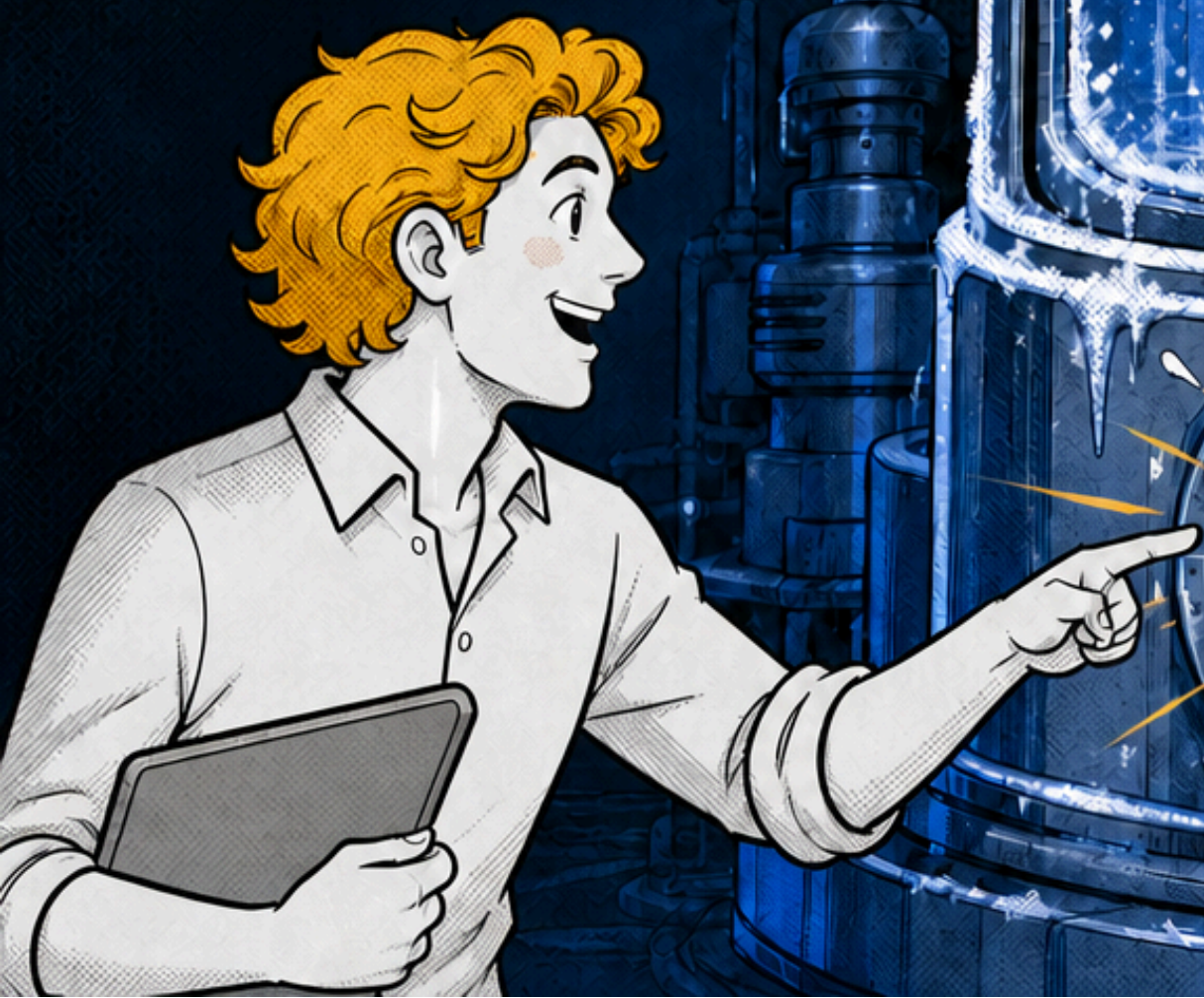
THE COLD REALITY OF QUANTUM HARDWARE

 Most superconducting quantum processors operate at around **0.015 Kelvin** — colder than outer space.

 Any heat, vibration, or electromagnetic noise causes a qubit to lose its quantum state.

 This process is called **decoherence**, and it's the central engineering challenge in the field.

 Once disturbed, the quantum state **collapses** and the calculation **falls apart**.



ERROR CORRECTION IS EXPENSIVE OVERHEAD

Even with extreme cooling, quantum gates are error-prone. Building one reliable logical qubit currently requires **dozens to thousands** of physical qubits correcting each other's errors.

Raw qubit counts have scaled through 2025–2026, but **qubit quality** — error rates and coherence time — matters as much as headline numbers.

The overhead remains substantial.

DOZENS TO THOUSANDS OF PHYSICAL QUBITS

THAT'S THE OVERHEAD.



LET ME COUNT... THAT'S A LOT.

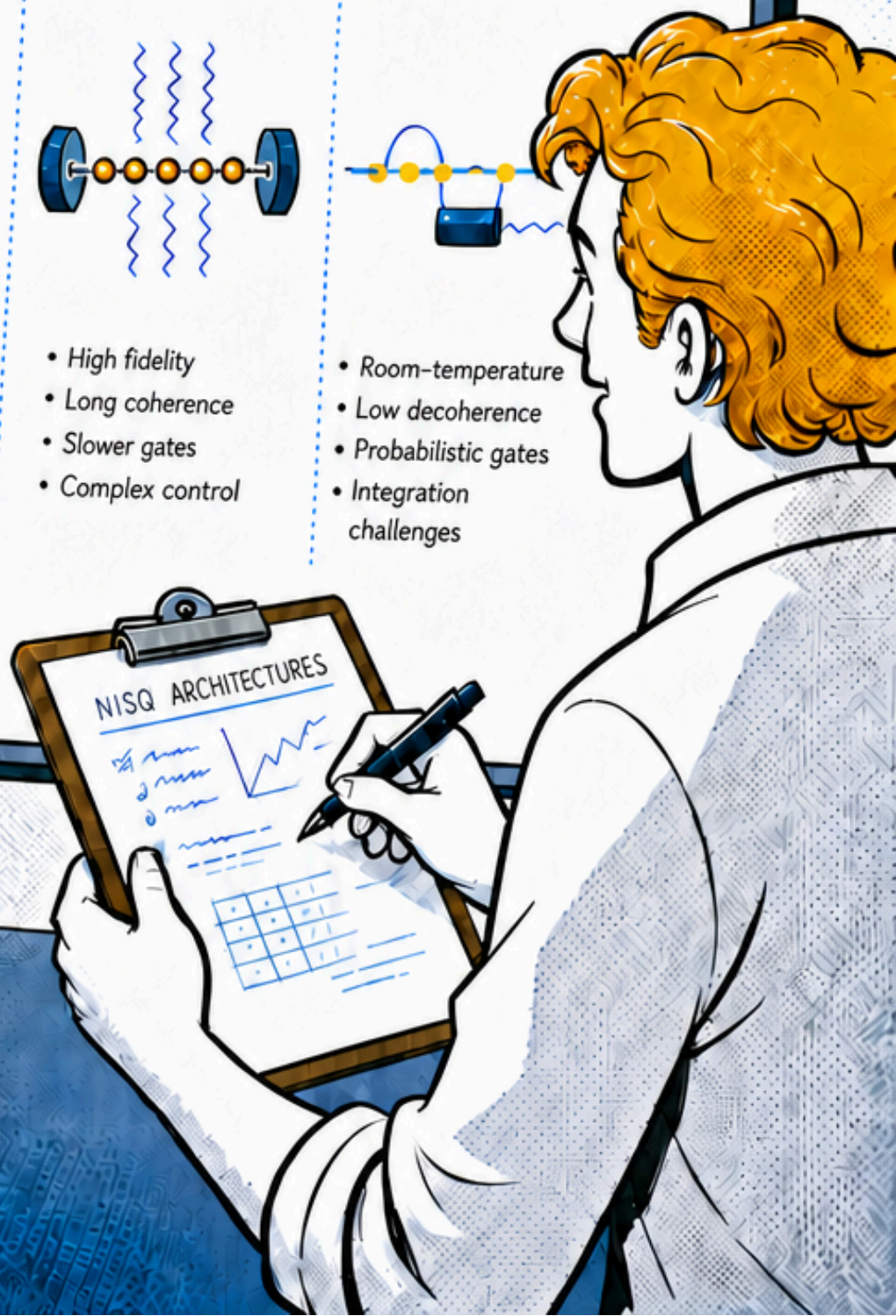
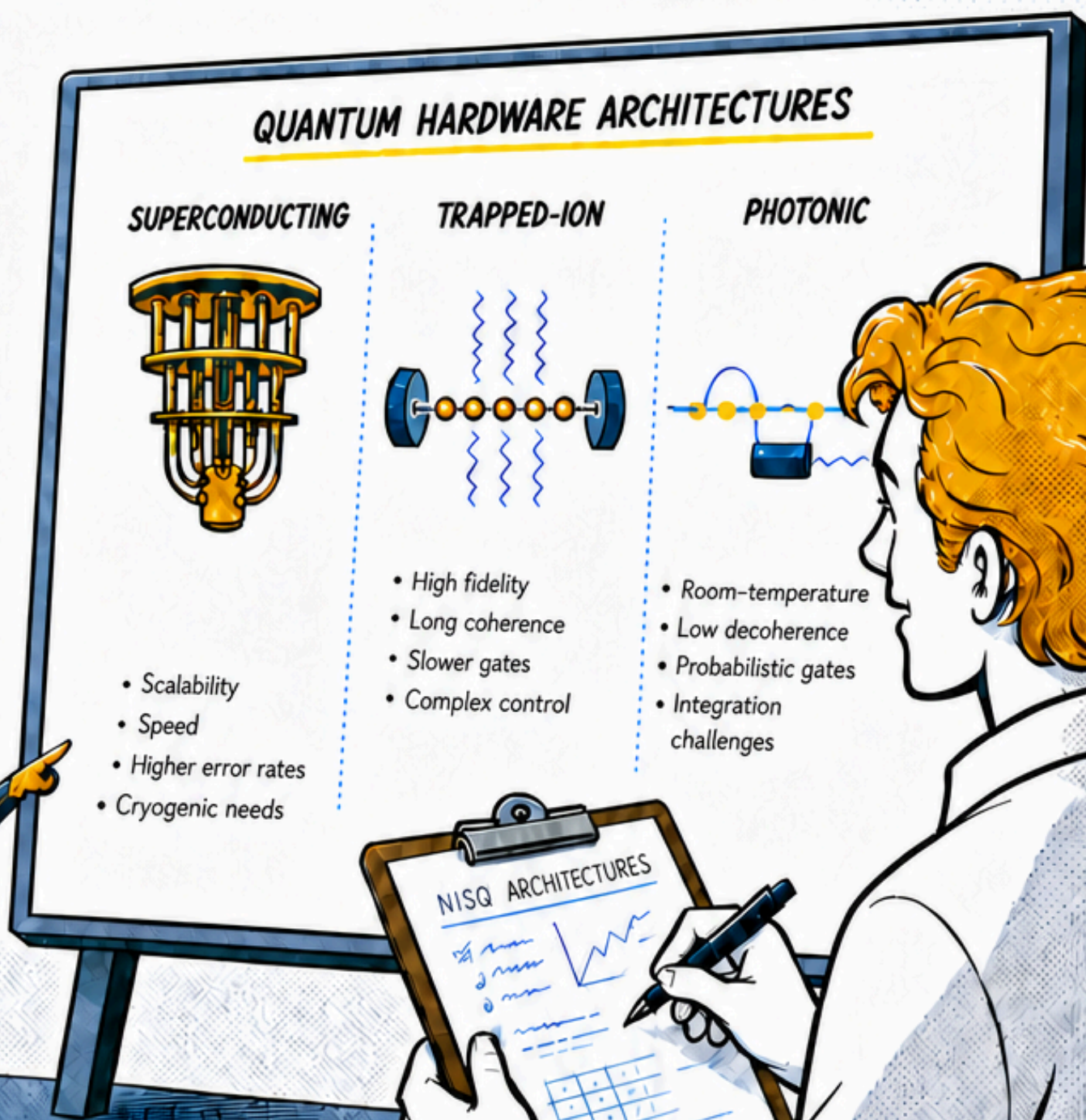


1 LOGICAL QUBIT



THE NISQ ERA: REAL, BUT LIMITED

Today's machines are called **NISQ** — Noisy Intermediate-Scale Quantum. They're genuine and improving, but not general-purpose replacements for classical computers. They're **specialised tools** with advantages only for specific problem classes. Superconducting, trapped-ion, and photonic architectures each carry different trade-offs.

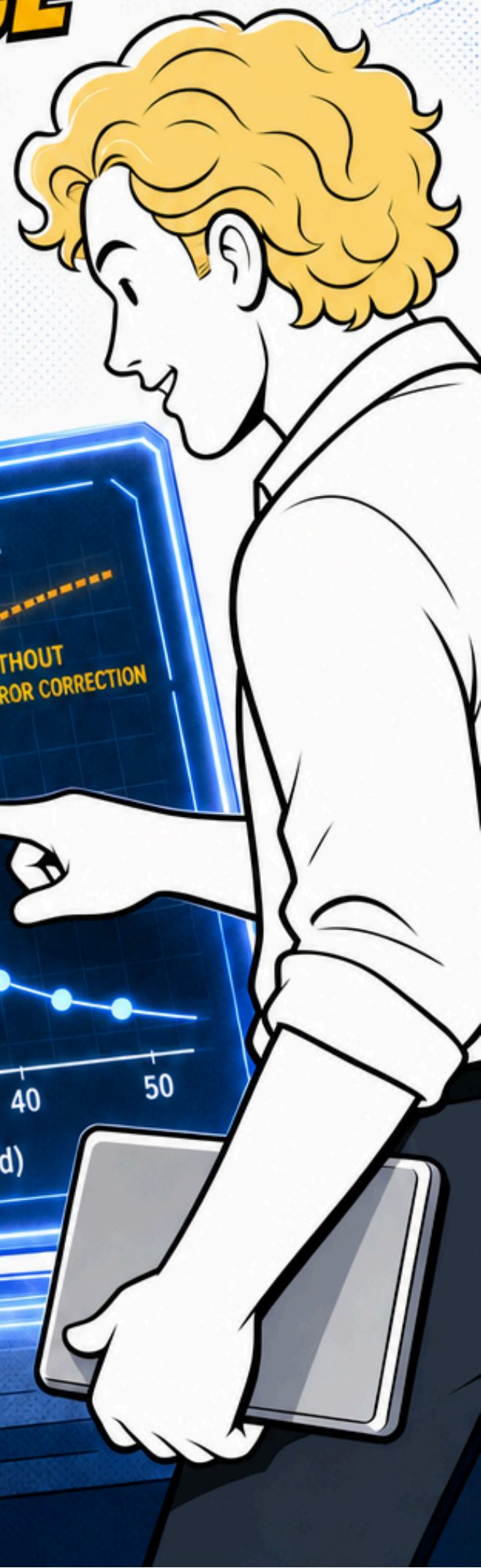
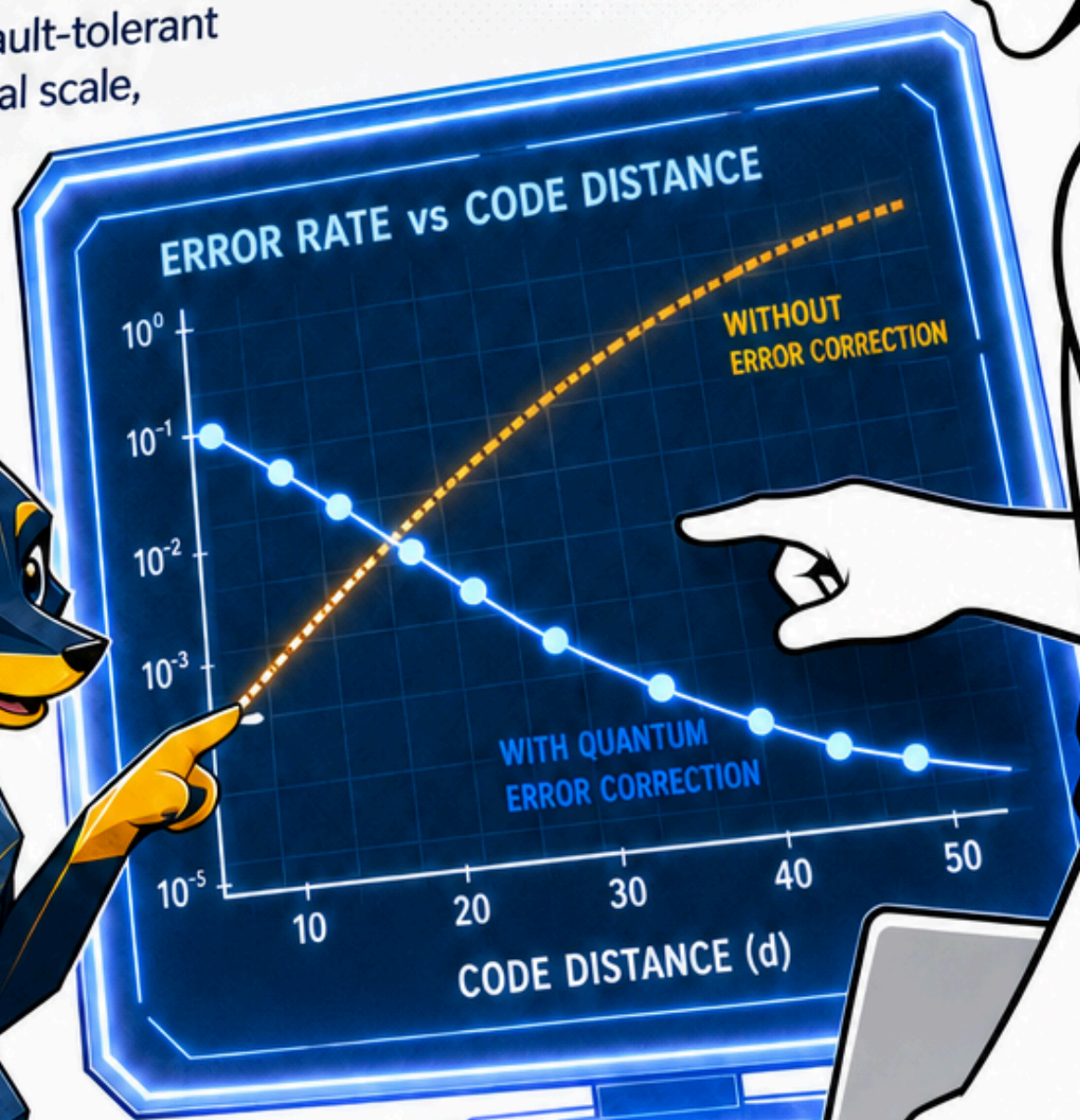


2026: FAULT TOLERANCE MOVES FROM THEORY TO PRACTICE

Google's Willow chip (Nature, December 2024) showed error rates **decreasing** as code distance increases — a landmark result.

In 2026, quantum error correction is crossing from theoretical goal to **engineering reality**.

A gap still remains before fault-tolerant machines operate at practical scale, but the trajectory is clear.

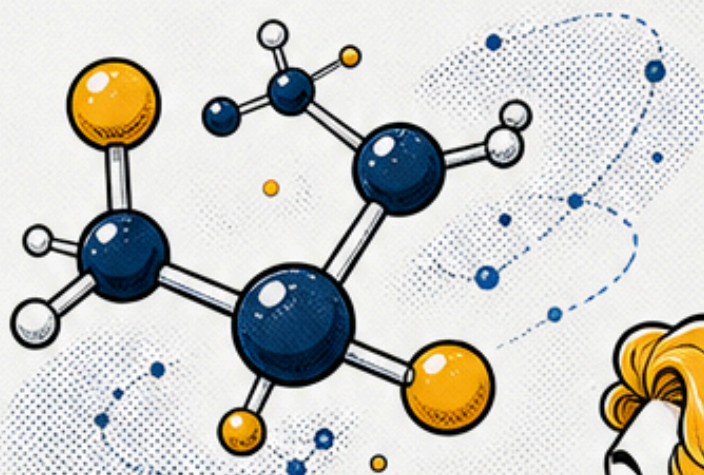


WHERE QUANTUM ADVANTAGE IS **ACTUALLY** EMERGING

So, which problems benefit first? Four areas stand out,
and they're not arbitrary.



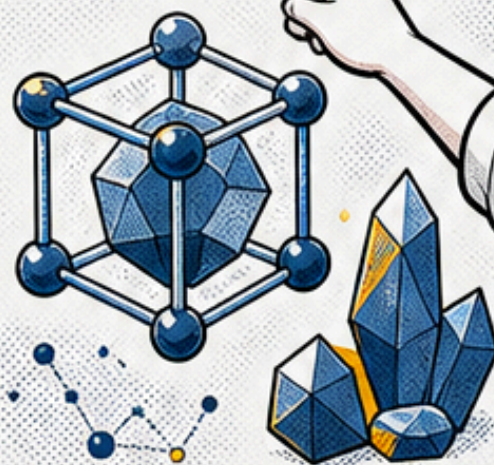
CRYPTOGRAPHY



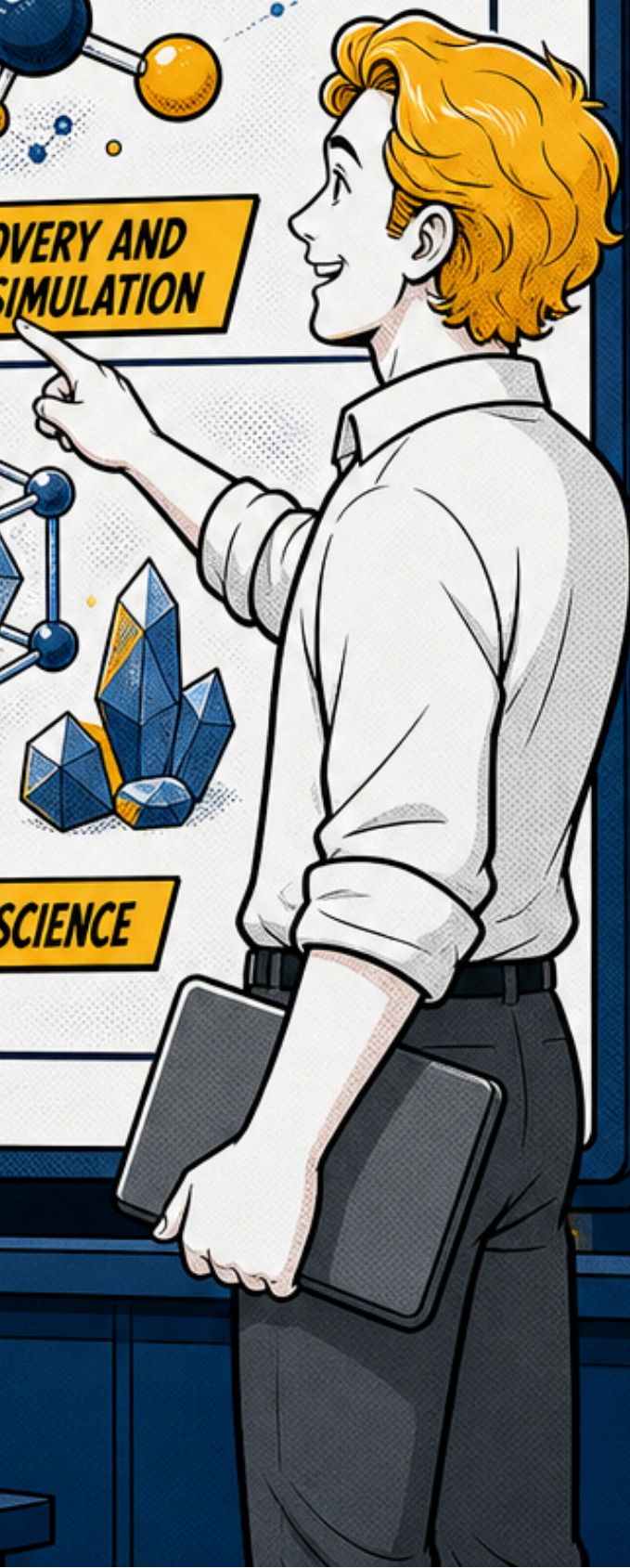
**DRUG DISCOVERY AND
MOLECULAR SIMULATION**



LOGISTICS OPTIMISATION



MATERIALS SCIENCE



CRYPTOGRAPHY

THIS IS THE **MOST URGENT** APPLICATION DOMAIN, AND THE PRESSURE IS REAL **NOW**, NOT IN TEN YEARS.

QUANTUM ALGORITHMS CAN **BREAK THE ENCRYPTION STANDARDS, LIKE RSA**, THAT CURRENTLY SECURE MOST OF THE WORLD'S FINANCIAL TRANSACTIONS, COMMUNICATIONS, AND DATA.



THE CONSEQUENCE IS A RISK CALLED "**HARVEST NOW, DECRYPT LATER**": STATE-LEVEL ACTORS ARE ALREADY COLLECTING ENCRYPTED DATA TODAY, WITH THE INTENTION OF DECRYPTING IT ONCE QUANTUM MACHINES BECOME POWERFUL ENOUGH.

G7 MEMBERS AND INTERNATIONAL STANDARDS BODIES ARE DEVELOPING FRAMEWORKS FOR **POST-QUANTUM TRANSITION**, PARTICULARLY IN FINANCIAL SERVICES.

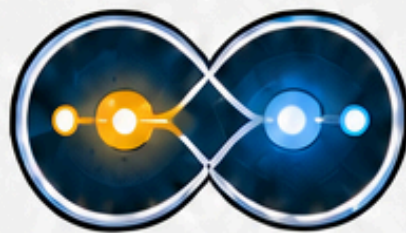
IN 2024, NIST FINALISED ITS FIRST SET OF **POST-QUANTUM CRYPTOGRAPHY STANDARDS**, INCLUDING ALGORITHMS DESIGNED TO RESIST QUANTUM ATTACKS. MIGRATION TO THOSE STANDARDS IS NOW UNDERWAY ACROSS CRITICAL INFRASTRUCTURE.



ENCRYPTED DATA



SECURE STANDARDS



QUANTUM KEY DISTRIBUTION

QUANTUM COMPUTING ALSO ENABLES A POSITIVE-SIDE CRYPTOGRAPHY APPLICATION: **QUANTUM KEY DISTRIBUTION**, WHERE ENTANGLED QUANTUM STATES ARE USED TO CREATE ENCRYPTION KEYS THAT ARE PHYSICALLY IMPOSSIBLE TO INTERCEPT WITHOUT DETECTION.



WHY MOLECULES NEED QUANTUM COMPUTERS

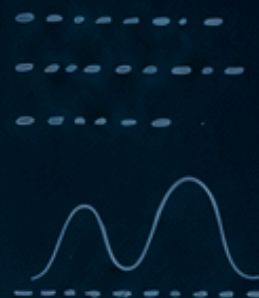
MOLECULES ARE QUANTUM SYSTEMS. PROTEIN FOLDING, ATOMIC INTERACTIONS, AND DRUG-RECEPTOR BINDING ARE FUNDAMENTALLY QUANTUM MECHANICAL.

CLASSICAL COMPUTERS RELY ON APPROXIMATIONS THAT DEGRADE AS MOLECULES GROW MORE COMPLEX, MAKING ACCURATE SIMULATION INCREASINGLY DIFFICULT.



$$\hat{H}\psi = E\psi$$

$$\psi(\vec{r})$$



$$e^{-r/a_0}$$

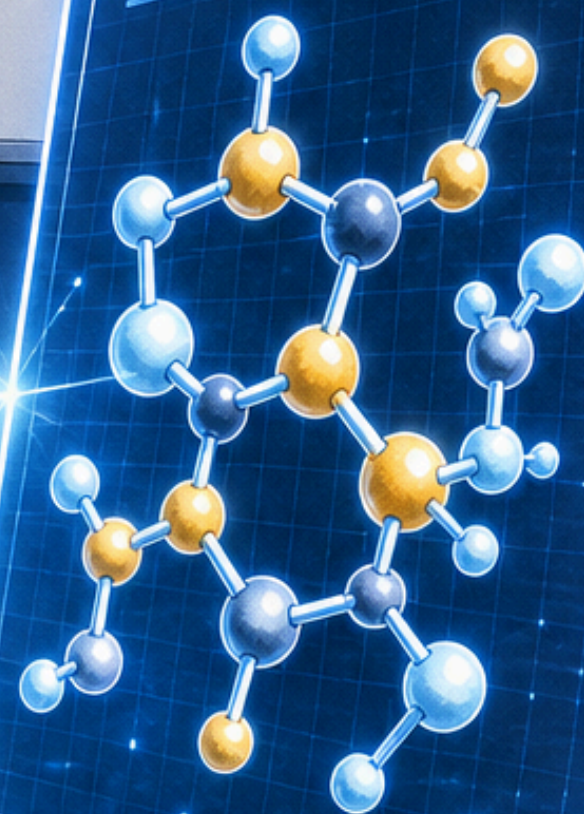
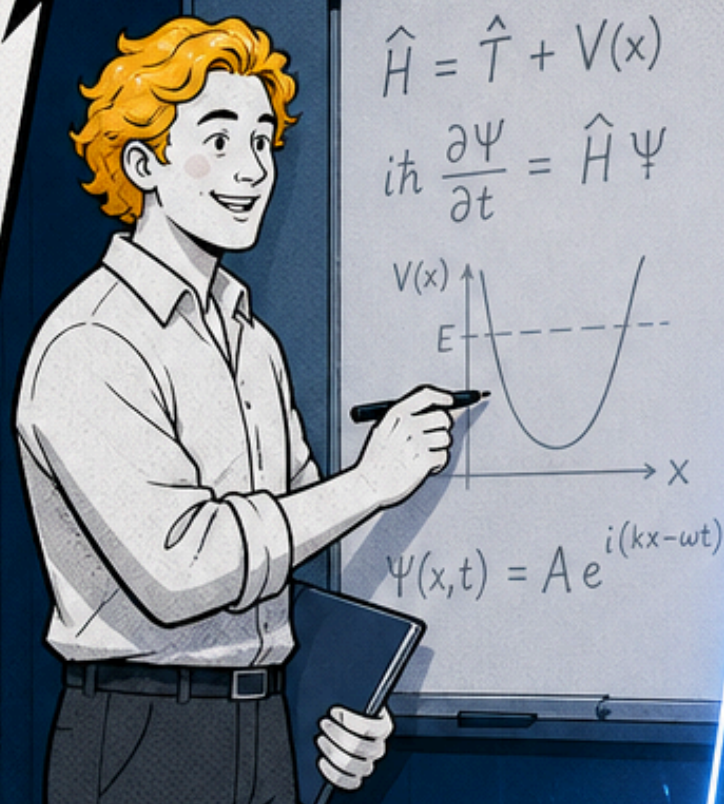
$$\hat{H} = -\frac{\hbar^2}{2m}\nabla^2 + V(r)$$



QUANTUM SIMULATION'S EDGE IN DRUG DISCOVERY

Quantum computers model molecular processes more directly, reducing approximation overhead.

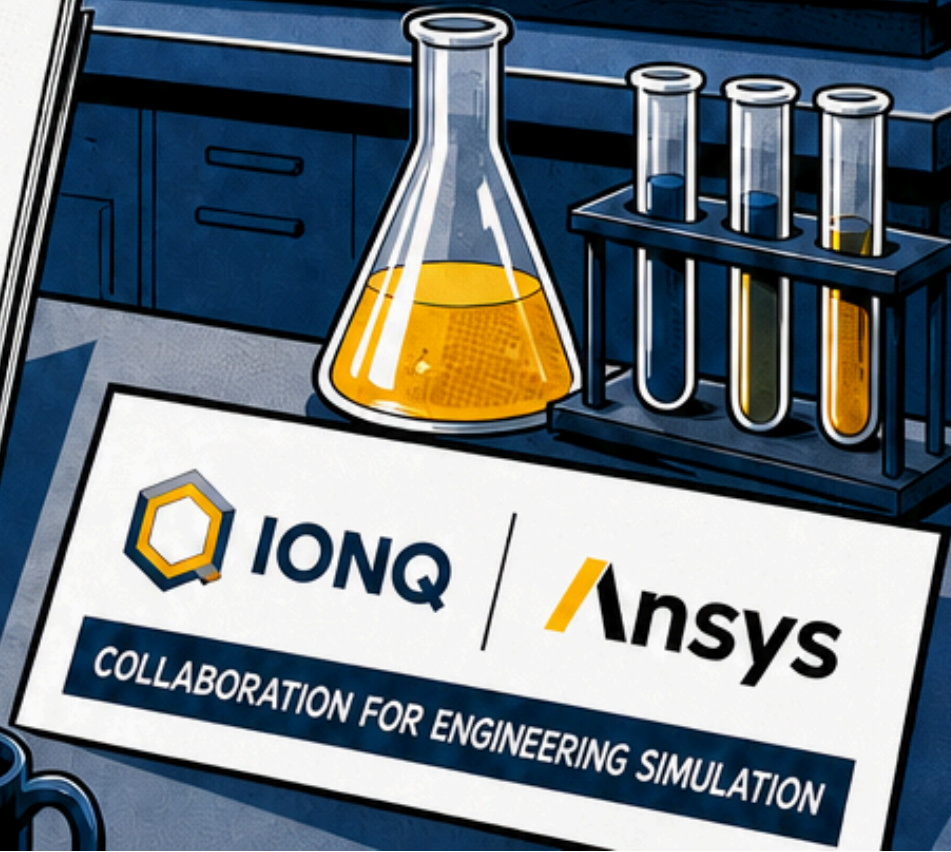
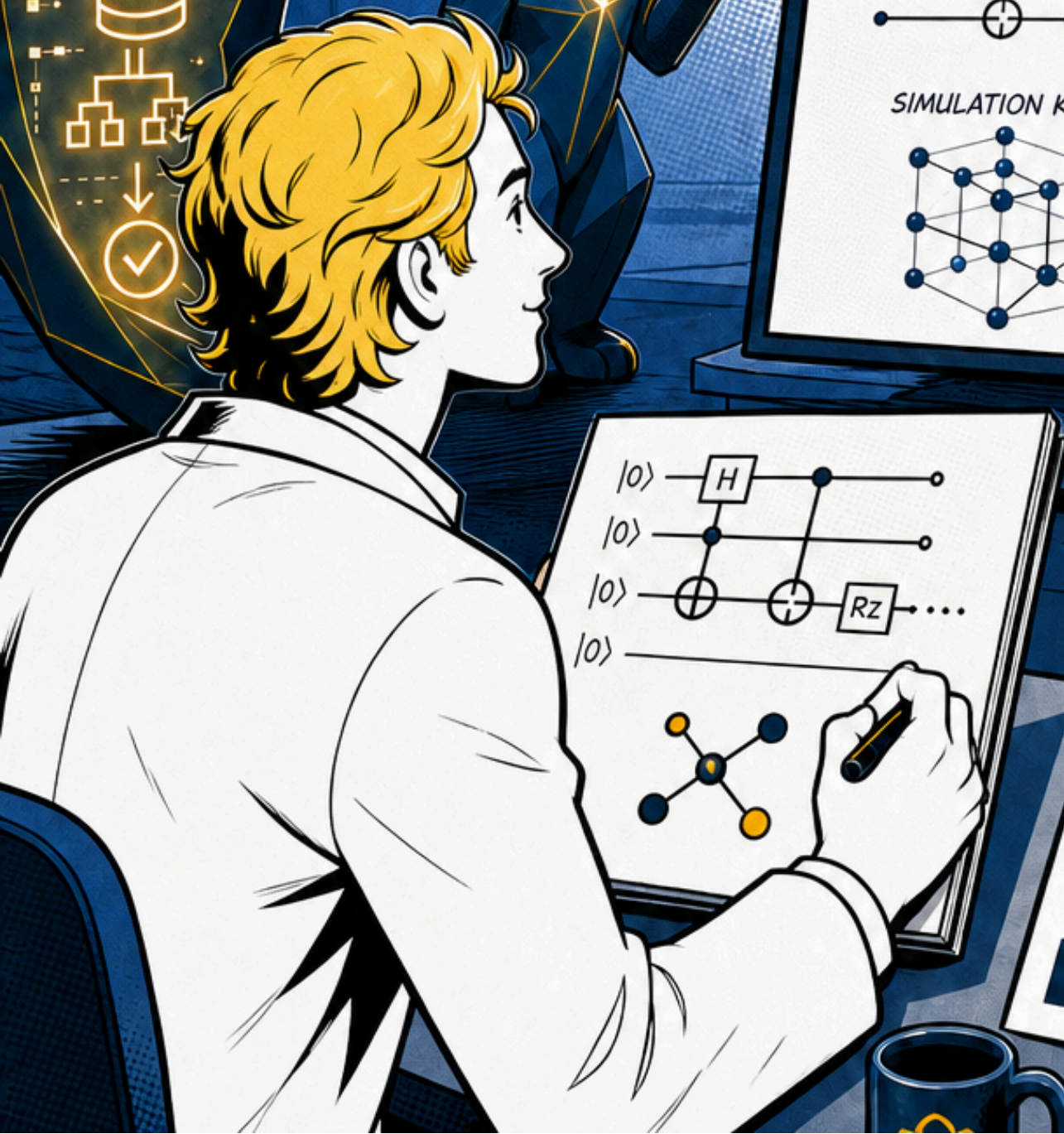
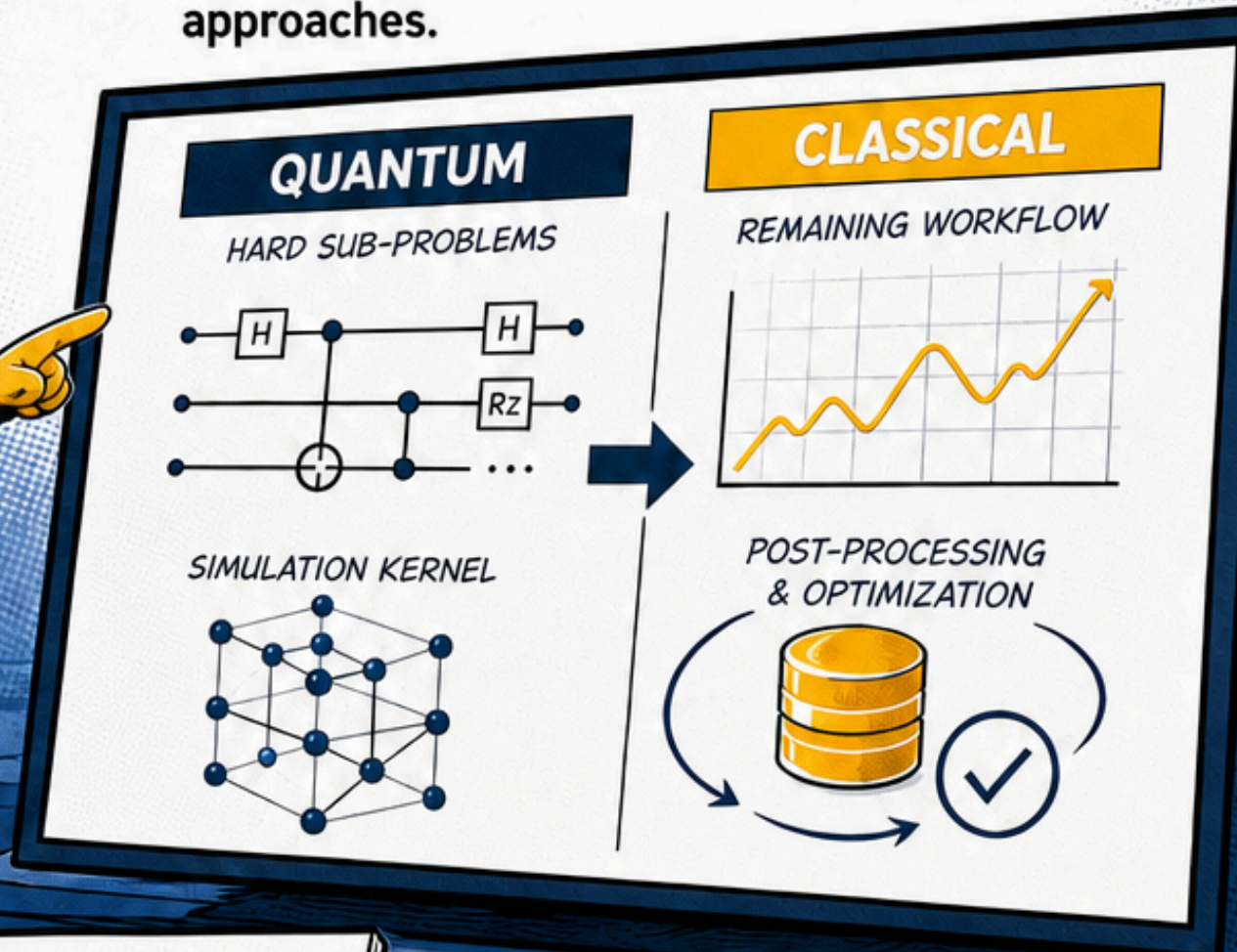
The payoff: shorter drug development cycles, faster identification of promising candidates, and access to protein structures too complex for classical methods to accurately resolve.



HYBRID WORKFLOWS AND INDUSTRY PILOTS

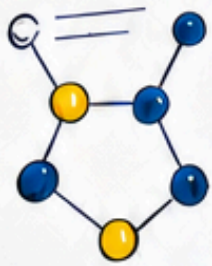
Pharma and materials science R&D are running early hybrid quantum-classical workflows, with quantum handling the hardest simulation sub-problems.

IonQ and Ansys announced a collaboration targeting engineering simulation, signaling growing real-world investment in these approaches.



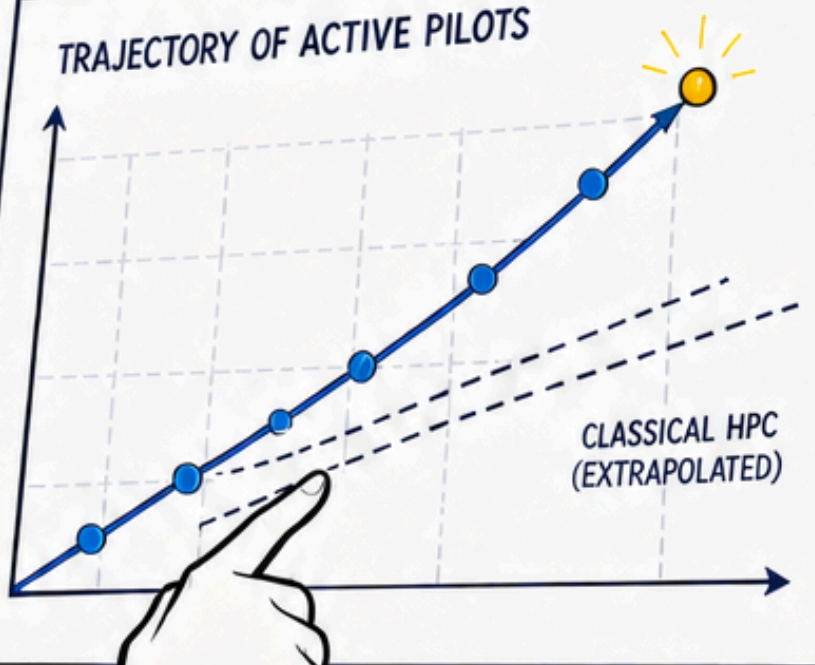
 **IONQ** |  **Ansys**
COLLABORATION FOR ENGINEERING SIMULATION

WHERE QUANTUM ADVANTAGE STANDS TODAY

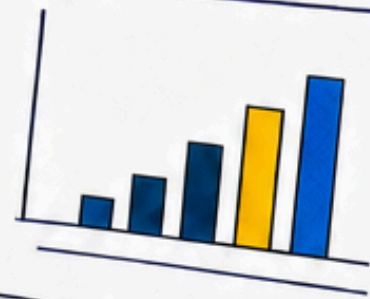
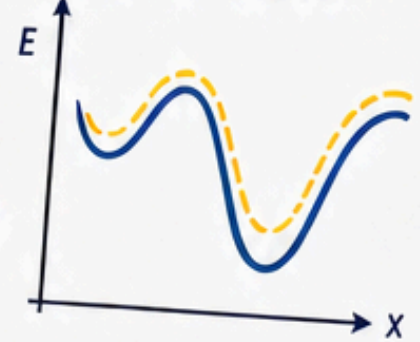


Documented cases of practical quantum advantage over classical HPC in molecular simulation remain limited and contested. Yet the trajectory of active pilots is being watched closely by researchers and investors alike, as the field edges toward meaningful breakthroughs.

TRAJECTORY OF ACTIVE PILOTS



ENERGY LANDSCAPE



LOGISTICS OPTIMISATION

ROUTE OPTIMISATION, SUPPLY CHAIN SCHEDULING, FLEET MANAGEMENT, ENERGY GRID BALANCING: THESE ARE ALL PROBLEMS WHERE THE NUMBER OF POSSIBLE COMBINATIONS EXPLODES EXPONENTIALLY WITH SCALE. CLASSICAL COMPUTERS HANDLE THEM WITH APPROXIMATION ALGORITHMS THAT FIND "GOOD ENOUGH" SOLUTIONS WITHOUT GUARANTEEING THE BEST ONE.

QUANTUM OPTIMISATION APPROACHES THE PROBLEM DIFFERENTLY, EXPLORING THE SOLUTION SPACE IN WAYS THAT MAY FIND BETTER ANSWERS AS THE PROBLEM SCALES.

LOGISTICS IS CURRENTLY ONE OF THE MOST ACTIVE AREAS FOR QUANTUM PILOTS, BECAUSE EVEN MARGINAL IMPROVEMENTS IN ROUTING EFFICIENCY AT SCALE TRANSLATE TO SIGNIFICANT COST SAVINGS.

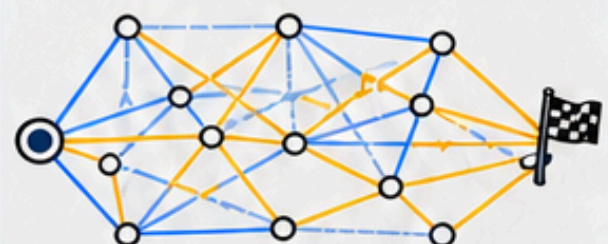


CLASSICAL APPROACH (APPROXIMATION)

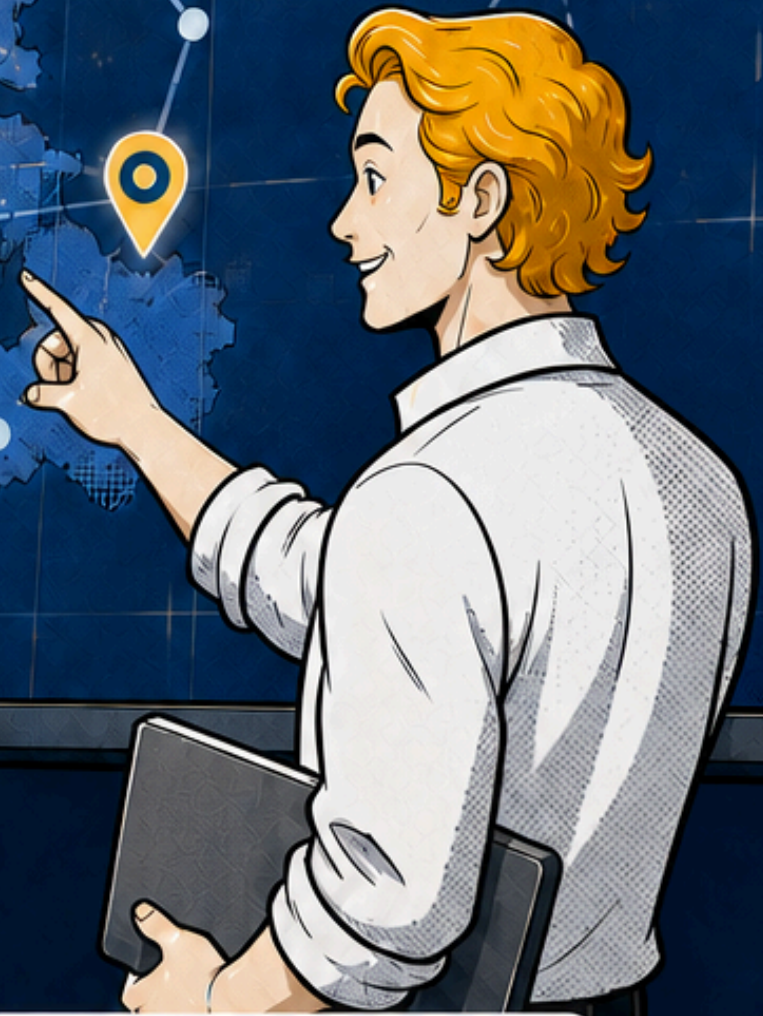


FINDS GOOD ENOUGH SOLUTIONS USING HEURISTICS.

QUANTUM APPROACH (EXPLORATION)



EXPLORES MANY POSSIBILITIES TO FIND BETTER ANSWERS AS PROBLEMS SCALE.



MATERIALS SCIENCE

Designing better batteries, stronger alloys, more efficient solar cells, or new superconductors all share a **common bottleneck**: we can't easily model how novel materials will behave at the atomic level using classical simulation. **Quantum simulation** is well suited to this problem, modelling atomic and molecular interactions with quantum-level precision rather than approximation.

Researchers have applied quantum simulation methods to longstanding materials science questions, including problems in quasicrystal structure and other areas where classical approximations have historically fallen short.

Battery development and semiconductor materials are now **high-priority application areas** for commercial quantum R&D.



WHAT THIS MEANS IF YOU'RE NOT A PHYSICIST

QUANTUM



Specialised for extremely hard problems



Potential within this decade



Cryptography



Pharma research



Logistics



Materials science



Practical impact in **specific** high-stakes domains

CLASSICAL



Optimised for everyday computing tasks



Excellent at what they're designed to do



✓ CRM

✓ Spreadsheets

✓ Email

✓ General software

✓ ...and more



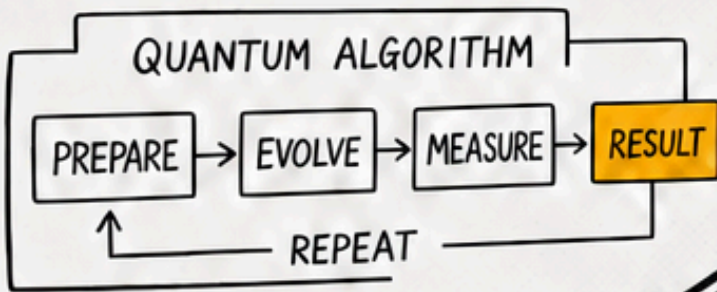
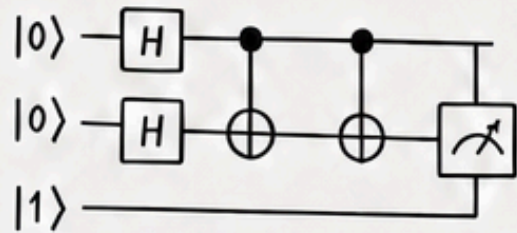
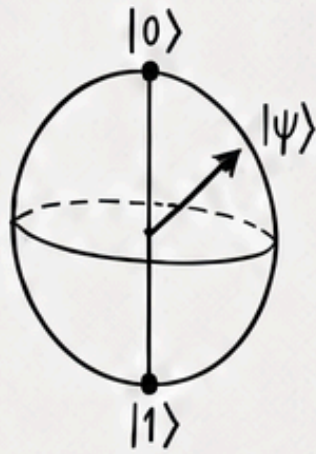
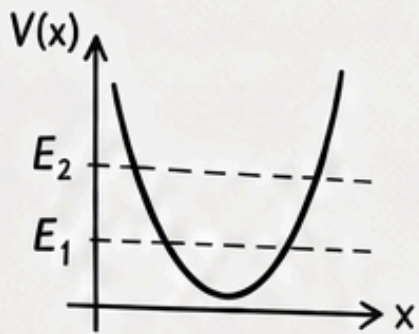
Reliable, mature, and irreplaceable for most workloads



UNDERSTANDING THE TECHNOLOGY CLEARLY IS THE STARTING POINT FOR UNDERSTANDING WHERE IT **INTERSECTS WITH YOUR BUSINESS.**

$$\hat{H} = -\frac{\hbar^2}{2m} \nabla^2 + V(x)$$

$$i\hbar \frac{\partial \psi(x,t)}{\partial t} = \hat{H} \psi(x,t)$$



EXPLAINING COMPLEX TECHNOLOGY IS A SKILL

that's where **infrairis** comes in



Don't
worry...We
can still
explain it!

