ENTRUST

SECURING A WORLD IN MOTION

ebook

Quantum Computing is Here

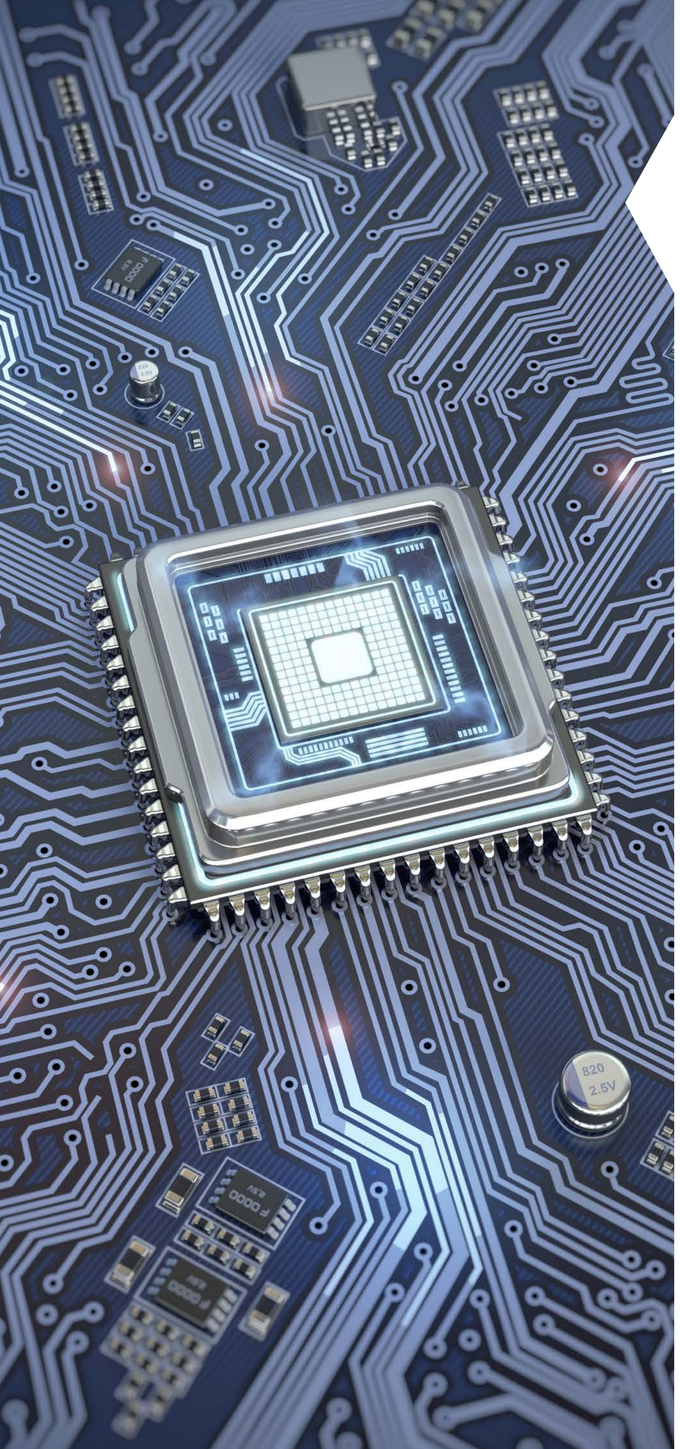
The State of the Quantum World and Cryptography

PART 1

Part 1 of a 3-Part Series That Answers:

1. What is a quantum computer?
2. When will quantum computers become mainstream?
3. How will quantum computers affect cryptography?

Table of contents



Quantum Computers Making Headlines

No doubt you're hearing about quantum computers in the news. Companies like IBM, Microsoft, and Google are all racing to build reliable quantum computers that promise to speed data transfers, enhance cryptography, and even predict more accurate weather forecasts. But what exactly is quantum computing? According to MIT, "a quantum computer harnesses some of the almost mystical phenomena of quantum mechanics to deliver huge leaps forward in processing power."

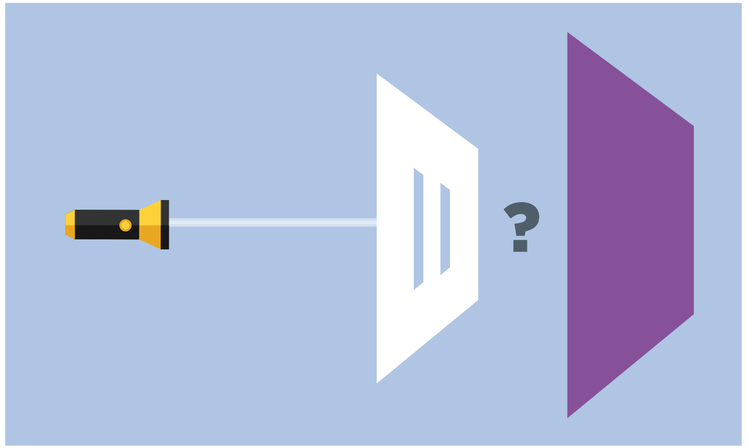
Quantum computers, when fully realized, are expected to be far more powerful than the traditional computers we use at work, at home, on a desk, or in our hands. These computers will be able to solve some problems faster than any current or emerging supercomputers – solving problems that would require 10,000 years on a supercomputer in just a few minutes.[1]

> **«Quantum computing is poised to upend entire industries – from telecommunications and cybersecurity to advanced manufacturing, finance, medicine, and beyond.[2]»**

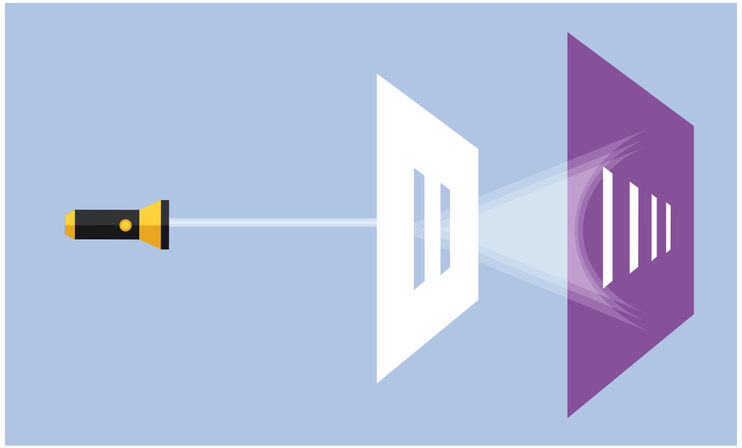
1 New York Times, Google Claims a Quantum Breakthrough That Could Change Computing, 2019
2 CBInsights, What is Quantum Computing?, 2019

Where Quantum Computing Began

To understand present-day and future quantum computers, we need to go back to where it all began in 1801. Physicist Thomas Young conducted a “double slit” experiment to answer the question: What is light – a wave or a particle?



Young hypothesized that light would go through the two slits of the metal plate and display two lines on the screen.



To his surprise, the light went through the two slits of the metal plate, but instead of displaying just two lines, it displayed many more lines on the screen.

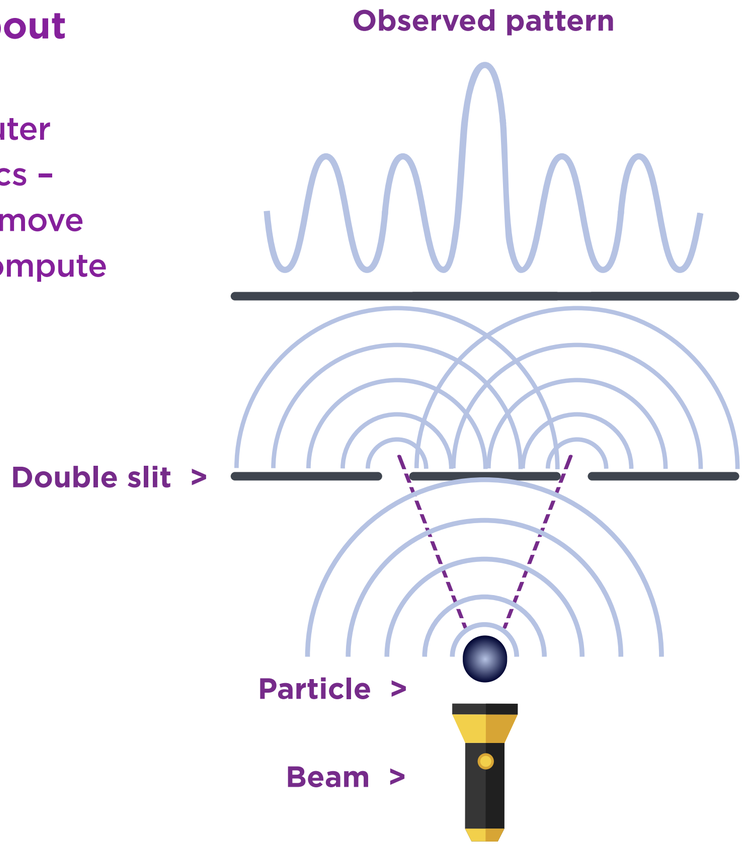
What’s Going On?

A photon is the smallest discrete amount – or quantum – of electromagnetic radiation that is produced by light. However, these photons move in waves. In Young’s experiment, when the light hit the two slits, it caused an interference pattern that created crests and troughs on the screen.

So, the answer to our earlier question? Light is both a wave and a particle.

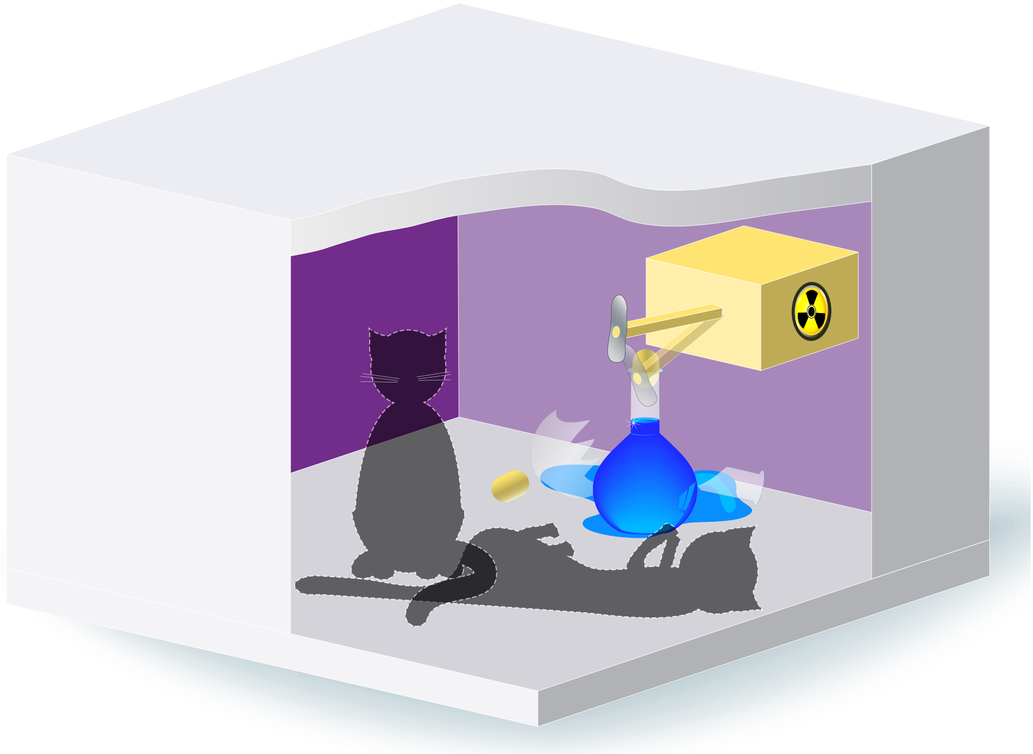
Why are we talking about lights and detectors?

Because a quantum computer exploits quantum mechanics – how particles interact and move at the smallest level – to compute its answers.



Applying Quantum Particles to the Macro World

In 1935, Aaron Schrodinger's famous thought experiment, now known as "Schrodinger's cat," introduced the concept of superposition at a macro level. Superposition means being in multiple states at the same time. He described a hypothetical cat in a metallic box with a vial of poison and a hammer attached to a Geiger counter, which would detect the decay of particles from a radioactive element and trigger the hammer to break the vial of poison. Therefore, the fate of the cat is tied to the quantum process of radioactive decay. The cat is alive when it enters the box and dead if the poison is unleashed.



However, without opening the box, you can't be sure if the cat is dead or alive – so the cat is in two states: superposition. Alive and dead at the same time!

How a Quantum Cat Relates to Quantum Computers

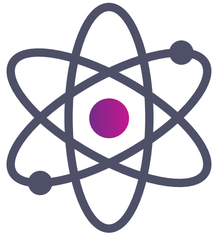
Qubits work on a quantum computer like bits work on a classical computer. They represent the smallest, finite unit of quantum computation done on a quantum computer. When in superposition, qubits are just like a subatomic quantum cat in both dead and alive states.

So, how do these computing processes compare?

"Classic Computer"

Works on "classical" bits

- Uses a memory made up of bits, either 0 or 1
- Can only exist in one state at a time
- Calculations performed by logic gate operations
- Single state bit order (10 bits in, 10 bits out)
- Deterministic solution – run algorithm and get same answer every time

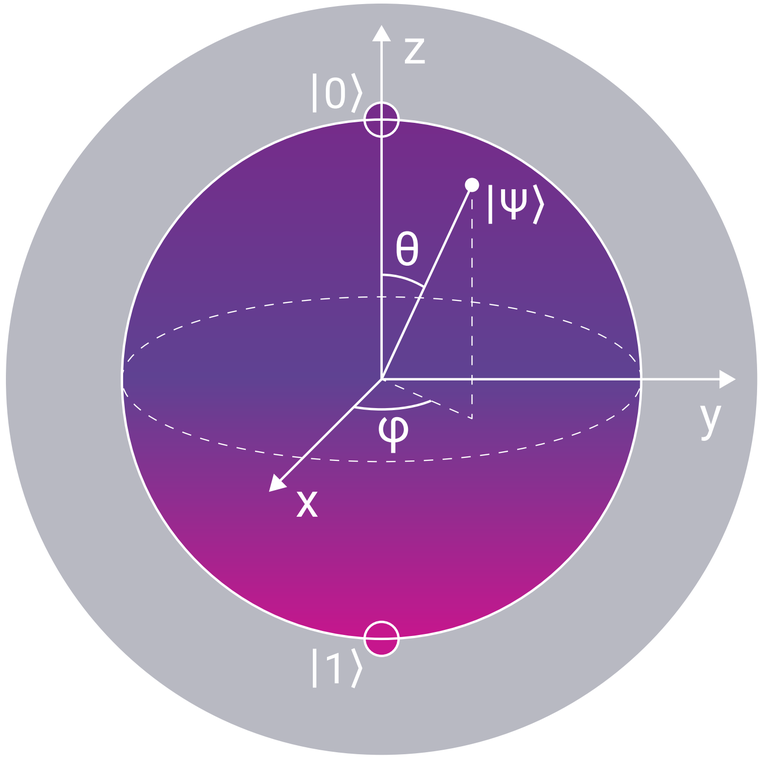


Quantum Computer

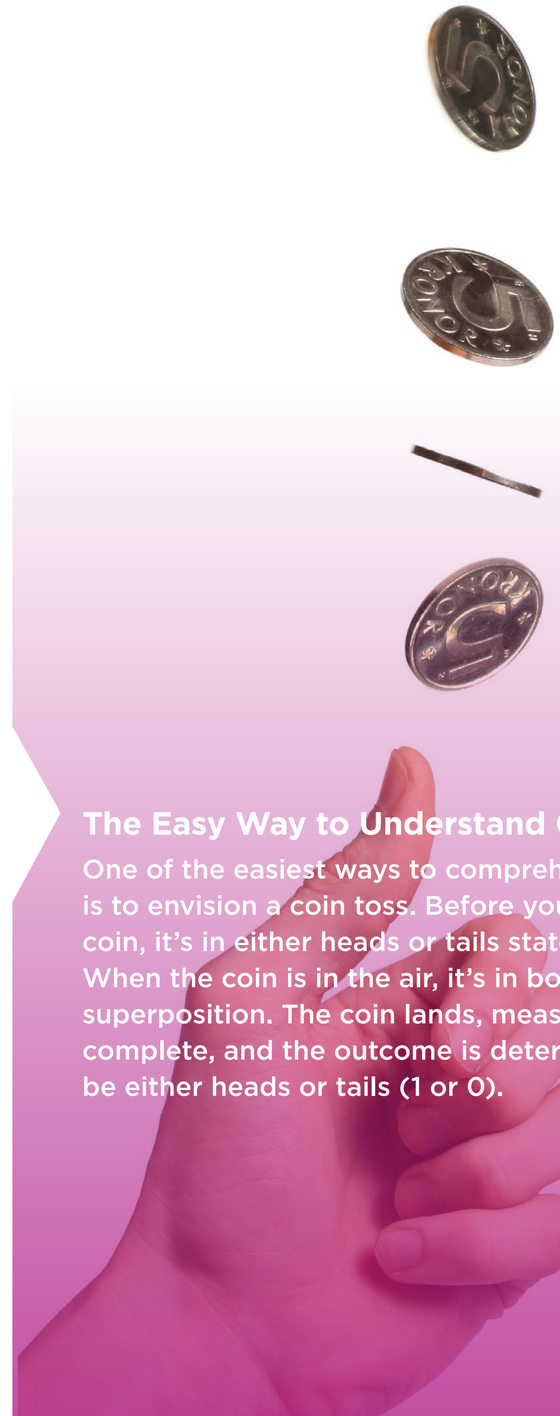
Works on qubits

- Can represent 0, 1, or any quantum "superposition" of the two states
- Each additional qubit can be in a superposition of 2^n states
- Problem is encoded into the qubits (via quantum gate operations)
- Calculation ends with measurement (open the box to see what state the cat is in) and causes the 2^n states to collapse back into one of the 2^n eigenstates (states of a quantized dynamic system), known as "collapse of the wave."

The Bloch Sphere Qubit Model



The Bloch Sphere was developed by Felix Bloch in 1935 as a model of a qubit. The north (|0>) and south (1>) poles of the sphere represent classical bits (deterministic) and the vectors inside the sphere represent all the possible superposition states of the sphere (probabilistic). After a quantum computation, the qubit will collapse to either of the poles based on the probability encoded into the superposition state.



The Easy Way to Understand Qubit

One of the easiest ways to comprehend qubit is to envision a coin toss. Before you flip a coin, it's in either heads or tails state (1 or 0). When the coin is in the air, it's in both states – superposition. The coin lands, measurement is complete, and the outcome is determined to be either heads or tails (1 or 0).

Quantum Computing's Impact on Society

Quantum computing has ushered in major change for society – impacting everything from artificial intelligence (AI) to chemistry, biology, and physics.

Financial Systems

Ability to model systems with more connections between them or look up more data.

AI

Emergence of deep learning systems to make more connections, enhance search, and apply quantum algorithms.

Chemistry/Biology /Physics

Opportunity to model bigger molecules, atoms, drug interactions, etc.

Cryptography

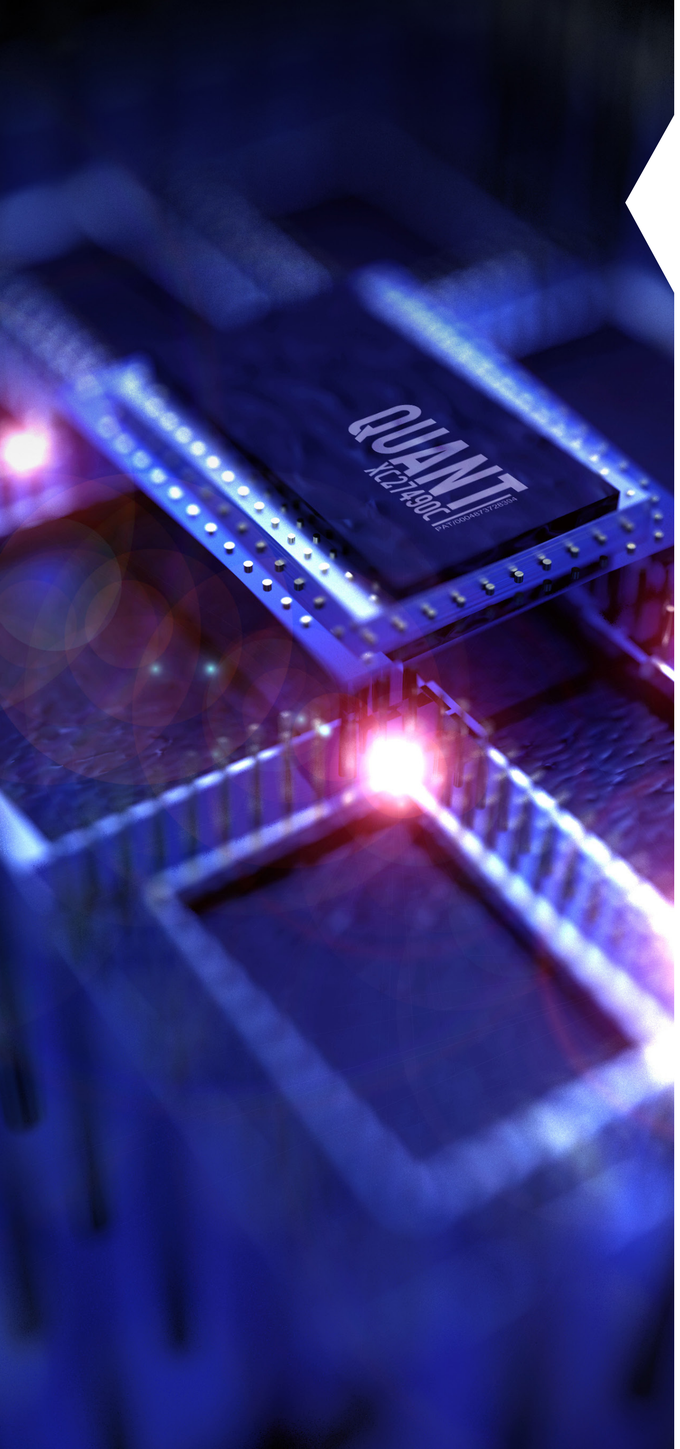
Factoring RSA keys and breaking the discrete logarithm problem (DLP) in elliptic curve cryptography (ECC) will be feasible.

Quantum Computing Compromises Crypto Security

There will need to be significant changes made to cryptographic security for quantum computing. While some cryptographic algorithms will remain secure, others will be at risk. For example, many e-commerce websites rely on vulnerable cryptographic schemes called public key cryptography. The most popular of these, RSA, is built on prime number factorization. These keys will be easily cracked by quantum computers because they can easily identify patterns in these algorithms.[3]

CRYPTOGRAPHIC ALGORITHM	TYPE	PURPOSE	IMPACT OF QUANTUM COMPUTING
AES-256	Symmetric Key	Encryption	Secure
SHA-256, SHA-3	–	Hash Functions	Secure
RSA	Public Key	Signatures, Key Establishment	No Longer Secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public Key	Signatures, Key Exchange	No Longer Secure
DSA (Finite Field Cryptography)	Public Key	Signatures, Key Exchange	No Longer Secure

3 Science magazine, Cryptographers scramble to protect the internet from attackers armed with quantum computers, 2019



Quantum Computers Are Already Mainstream

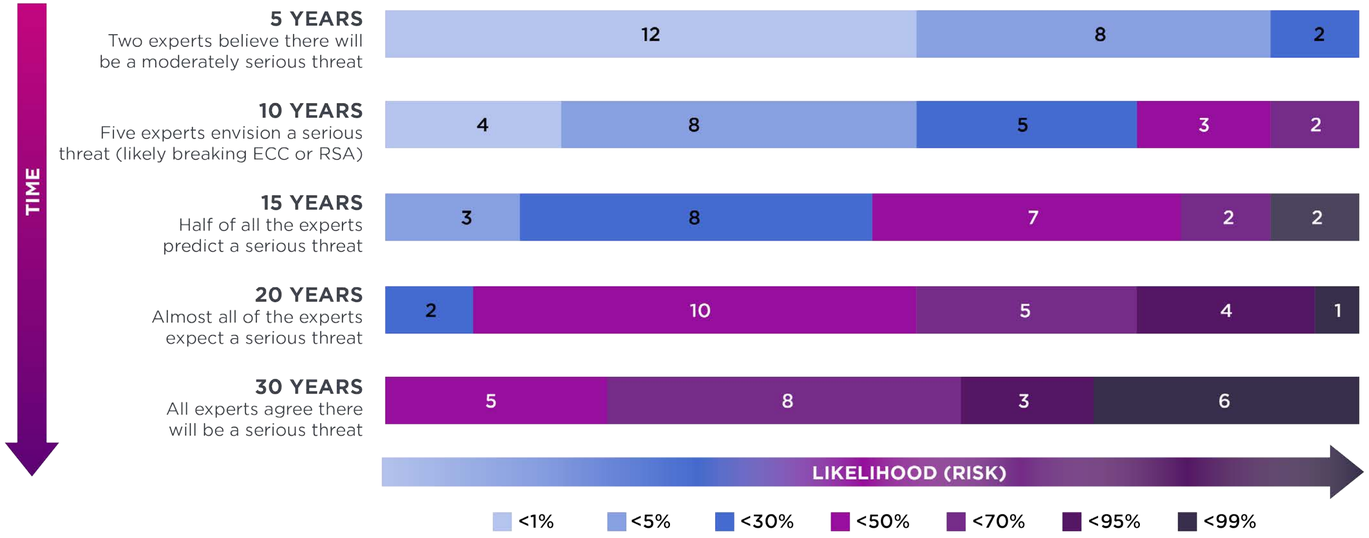
While quantum computing has entered the mainstream, the systems available today are still rudimentary, compared to where they may yet end up. Many of the industry's biggest players are focused on advancing quantum computing to the next level.

IBM	Microsoft	Google	D-Wave The Quantum Computing Company™	Honeywell
Unveiled a 127-bit qubit computer in 2021, with plans to launch a 433-qubit computer in 2022 and a 1,121-qubit computer in 2023.	Announced quantum supremacy – in a race with IBM to claim the title.	Introduced a topological method to create more stable quantum computers.	Has been offering quantum "annealing" computers for almost a decade.	In 2020, Honeywell built a quantum computer with a "Quantum Volume" of 64, considered the most capable at the time.

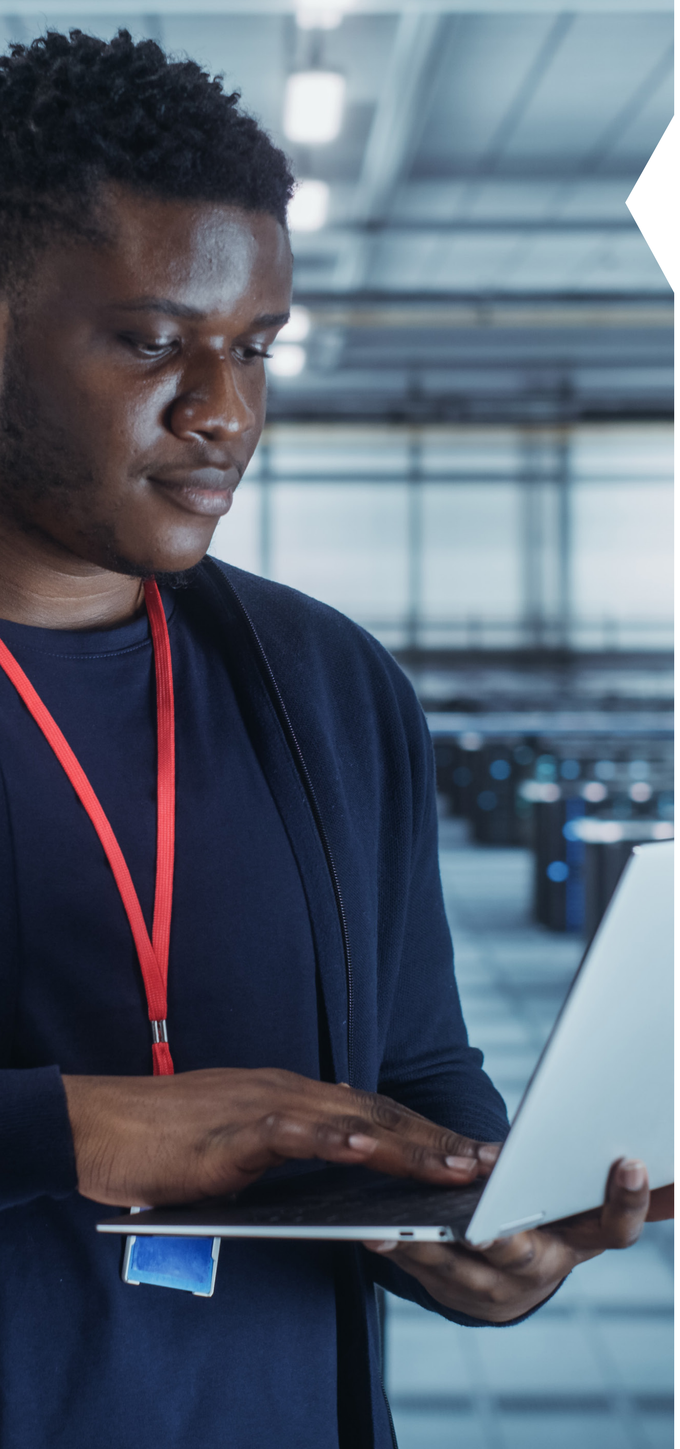
Cybersecurity Threats Are Coming – But How Fast?

There's no doubt that quantum computing will create threats to public key cryptography. Cybersecurity threat experts Evolution Q, working in coordination with the Global Risk Institute, conducted a survey with 22 cybersecurity experts to assess cybersecurity risk over the next 30 years.

Expert Opinions on the Likelihood of a Significant Quantum Threat to Public-Key Cybersecurity as Function of Time



Numbers reflect how many experts (out of 22) assigned a certain probability range.



Preparing for Quantum Computing Threats

Based on predictions from experts including the Global Risk Institute, it is expected that sometime between 2027-2033 something related to quantum computing will compromise security. National Institute of Standards and Technology (NIST) standards are not expected until 2022/2023. Therefore, the time is now to get ahead of this threat and secure your most important systems.

No one algorithm will protect against all the threats posed by quantum computing. To prepare, we need new algorithms – with different performance characteristics.

Types of cryptography that may be more resistant to quantum computing attacks:

- **Hash-based signatures**
- **Lattice-based crypto**
- **Supersingular isogeny DH**
- **Code-based crypto**
- **Multivariate polynomials**
- **Zero knowledge proofs**

Fact or Fiction – Sorting Through the Hype

There's a lot of hype around quantum computers today, but many organizations still aren't sure how it will impact their organizations and systems. Here are some of the facts – and fictions – surrounding quantum computing.

Q: Quantum computers will one day replace classical computers.

A: **Fiction.** Quantum computers will always work in tandem with classical computers. The process begins by preparing and massaging data in a classical computer, then it is passed off to the quantum computer.

Q: More qubits make a better quantum computer.

A: **Fiction.** A problem with quantum computers is noise (decoherence). With a noisy qubit, there is low probability to get to the right results. There aren't any fault-tolerant qubits today and larger systems will need even more fault-tolerant qubits for error correction.

Q: Quantum supremacy has been achieved.

A: **Maybe.** Google developed a problem that only a quantum computer could solve in an efficient way. It was a random number sampling algorithm and Google claims it was able to solve it in 200 seconds. IBM disputes this.

Q: I need to start thinking about how to protect my digital information from quantum computers.

A: **Fact.** Organizations should start assessing what types of cryptographic systems are in place today – and whether they need to transition to quantum -esistant cryptography.

Learn what your organization should do to prepare for quantum computing and post-quantum cryptography.

Contact info@entrust.com today.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223