Image source: iStock/Ankabala

Quantum computing, the next technology revolution?

After AI, quantum computing? Marketed as the next technological revolution, this emerging industry could reach a market value of $1.3 trillion by 2035, analysts say.

Google's quantum chip, Willow, can solve in under five minutes a problem that would take the fastest supercomputers 10 septillion years—longer than the universe's history. While not a replacement for everyday laptops, its potential in medicine, logistics, and materials science is groundbreaking.

This article offers a glimpse into the world of quantum computing, explores the emerging quantum companies driving change, and addresses one of its most debated questions: is quantum computing a threat for cryptocurrencies?

Jakub Dubaniewicz
Senior Equity Analyst

Assia Driss
Junior Investment Analyst

SYZ PRIVATE BANKING

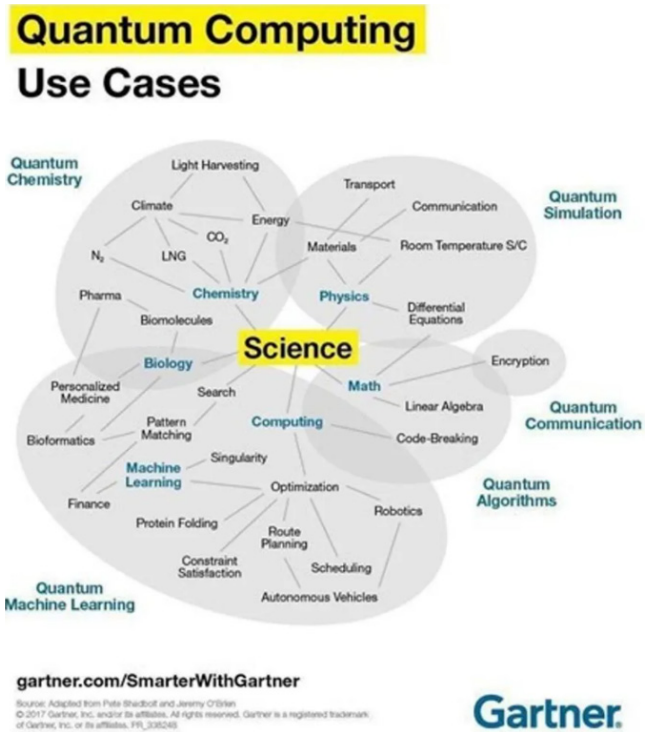
What is quantum computing?

Quantum computing is a form of computation that leverages the principles of quantum mechanics, a branch of physics governing the behaviour of particles at the atomic level. While a regular computer, like a laptop, uses bits, either 0 or 1, to process information, a quantum computer uses quantum bits (qubits), which can represent 0, 1 or a combination of both (00, 01, 10, 11), thanks to a property called superposition. This unique feature enables quantum processors to handle vast amounts of data at speeds exponentially greater than most advanced computers. In superposition, qubits scale exponentially: two qubits can process four pieces of data, three can process eight, four can process sixteen, and so on.

To put it in layman's terms, Timothy Hollebeek, Industry Standards strategist at DigiCert, imagines a labyrinth. A classical computer would methodically explore one path at a time to find the exit. A quantum computer, however, evaluates all possible paths simultaneously, delivering a solution far more quickly.

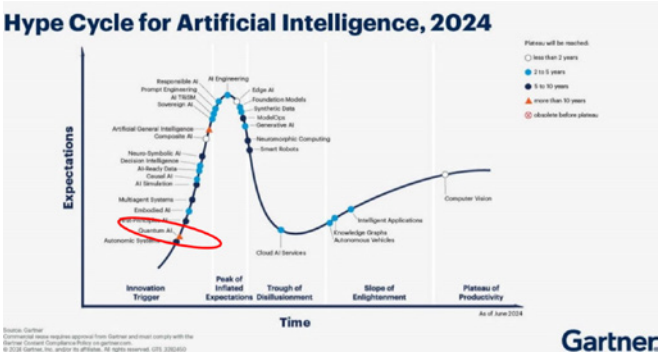
Qubits are interconnected through a phenomenon called entanglement, where the state of one qubit is directly linked to another, regardless of the distance between them. Quantum computers also leverage interference patterns to enhance correct results and suppress incorrect ones.

By combining superposition, entanglement, and interference, a quantum computer has the potential to factor large amounts of data and solve exceptionally complex problems. In medicine, quantum computers could discover new treatments by identifying patterns in clinical trial data or genetic information that are beyond the capabilities of current computational systems. They could also enhance the safety of AI-driven systems, including those used in military targeting, banking, and autonomous vehicles.



Source: Gartner

However, building a fully operational quantum processor requires first overcoming technical challenges. A practical quantum system would need thousands of stable and interconnected qubits. Google's Willow, for example, operates with 105 qubits, but even creating a single qubit is an immense engineering feat. Qubits only function at ultra-low temperatures, close to absolute zero, where certain materials become superconductors, eliminating electrical resistance. Furthermore, controlling and manipulating qubits to extract data is equally challenging. It requires atomic microscopes, ultra-precise lasers, and highly sensitive sensors. Even under ideal conditions, qubits are incredibly fragile and prone to disturbances or "noise." This noise can stem from factors like imperfections in manufacturing, fluctuations in control signals, temperature changes, or interactions with the surrounding environment. Such disturbances compromise the reliability of qubits. To illustrate the magnitude of the challenge: it took only 100 microseconds for Google's Willow to lose its quantum state, start interacting with its environment, and lose information. For quantum processors to perform meaningful computations, they need qubits with high fidelity that remain stable long enough to process data.



Source: Gartner

Quantum companies

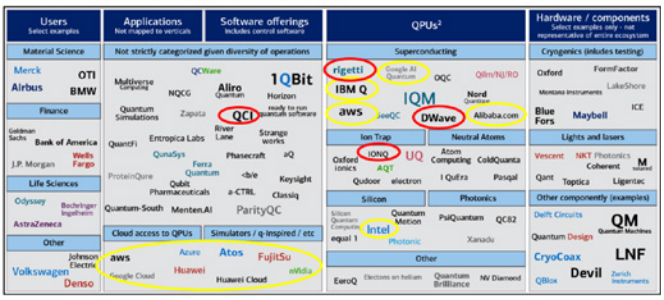
Quantum computing is considered to be at its infancy stages. The major focus of research has been on enhancing qubit stability and minimising errors. Big tech companies such as Google, IBM, Microsoft, and Amazon, alongside ambitious start-ups like Rigetti and IonQ, are driving the change by developing prototypes and investing heavily in quantum technology, making quantum computing a nascent yet highly promising area for investors. Many investors have high hopes that quantum computing sector could become the next tech revolution, mirroring the AI frenzy sparked by ChatGPT. Analysts estimate that quantum computing could become a $1.3 trillion industry by 2035.

By 2030, Google plans to build a full-scale quantum computer for $1 billion, its executives call it a small price for technology that could cure cancer. Following the announcement of its Willow quantum AI chip, a breakthrough in its research journey that began in 2012, Alphabet's stock rose by 5% on the day of the announcement and generated interest in pure-play investment options in quantum technology. Rigetti Computing (RGTI, 1210% rally over the past three months), IonQ Inc (IONQ, 217%), D-Wave (QBTS, 568%), and Quantum Computing Inc. (QUBT, 1344%) have all seen remarkable gains.

These relatively smaller companies, of which many were valued under $1 billion just months ago, are particularly prone to speculative interest and sharp market movements. Social media buzz, including Elon Musk's public congratulations and exchanges with Google's CEO, fuelled positive PR and investor enthusiasm, contributing to the rapid price increases.

However, many investors and scientists alike have warned that the development of large-scale, fault-tolerant quantum computers remains a distant goal, and that it may be too premature to identify winners in the sector and practical real-world use cases. Nvidia CEO Jensen Huang echoed this sentiment during a Q&A session at Nvidia's analyst day, stating that quantum computing might not have "very useful" applications for another 15 to 30 years. His remarks triggered a sharp sell-off in the sector, with Rigetti dropping 45%, IonQ losing 39%, D-Wave shedding 36%, and Quantum Computing Inc. falling 43% on Wednesday.

Exhibit 64: Quantum computing eco-system
Many companies, mainly private, comprise the quantum computer eco-system.



Source: BofA Global Research

A Threat to Crypto

Quantum computing, despite its incredible potential, casts a long shadow over the world of cryptocurrencies. The foundations of blockchain security may not be as unshakable as they seem.

While Google's Willow quantum computer, with its 105 qubits, remains far from the 1536–2338 qubits estimated to crack bitcoin's encryption, the rapid pace of research and development suggests that this once-distant threat is inching closer. The question is no longer if it will impact cryptocurrencies, but when.

The security of cryptocurrencies relies on public and private keys. Today, it is practically impossible to derive a private key from a public one using classical computers, but quantum computing's ability to process large amounts of data and factor large numbers could make this barrier obsolete. Some estimates predict that a well-functioning quantum computer could crack bitcoin's encryption in under 30 minutes. For an industry worth over $1.84 trillion, this is a chilling prospect. If quantum computers gain the upper hand, private keys could be exposed, wallets emptied, and the trust underpinning cryptocurrencies shattered.

The threat doesn't stop there. Blockchains themselves, known for their immutability and distributed security, could also be vulnerable. Bitcoin's decentralised network relies on the proof-of-work mechanism where immense computational power is required to maintain its integrity, but a sufficiently advanced quantum computer could overwhelm the system, rewriting transaction histories and seizing control. Quantum computing has the potential to cause the very structure of blockchain networks to crumble.

But all is not lost. The cryptocurrency world is not standing still. Developers are already discussing protocol upgrades to protect bitcoin against quantum threats. When solutions become clearer, a Bitcoin Improvement Proposal (BIP) will be published online for further debate and testing. If approved by the community and adopted by a majority of bitcoin nodes, it will be incorporated into the protocol.

Meanwhile, "quantum-safe" cryptography is emerging. One existing project is Quantum Resistant Ledger (QRL), a blockchain protocol built to withstand quantum attacks. At its core is the eXtended Merkle Signature Scheme (XMSS), a digital signature system akin to a single use lock that quantum computers cannot easily crack. With every transaction, a new, one-time signature is created, ensuring that even the most advanced quantum processors would struggle to hack.

It should be noted that quantum computing poses a threat not only to cryptocurrencies but to all systems relying on traditional encryption methods, including e-commerce platforms, banks, and government institutions. Tech leaders are stepping up. To date, IBM developed two post-quantum cryptographic algorithms, released by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST). Last February, Apple announced its intention to introduce quantum encryption measures to strengthen the security of data exchanged via iMessage. The race between quantum computing and cryptographic security is far from over, it is just beginning.

Conclusion

The technology is still far from being mature, and the road to practical, fault-tolerant quantum computing remains steep, but its arrival is inevitable. The challenges are significant—technical difficulties, scalability, security threats, and cost—but so are the opportunities. Quantum computing holds the potential to transform industries such as medicine, logistics, materials science and beyond. As Confucius' quote goes: "When the wind of change blows, some build walls, and others build windmills".

Welcome to Syzerland®

For further information

Banque Syz SA
Quai des Bergues 1
CH-1201 Geneva
T. +41 58 799 10 00
syzgroup.com

Jakub Dubaniewicz
Senior Equity Analyst
jakub.dubaniewicz@syzgroup.com

Assia Driss
Junior Investment Analyst
assia.driss@syzgroup.com