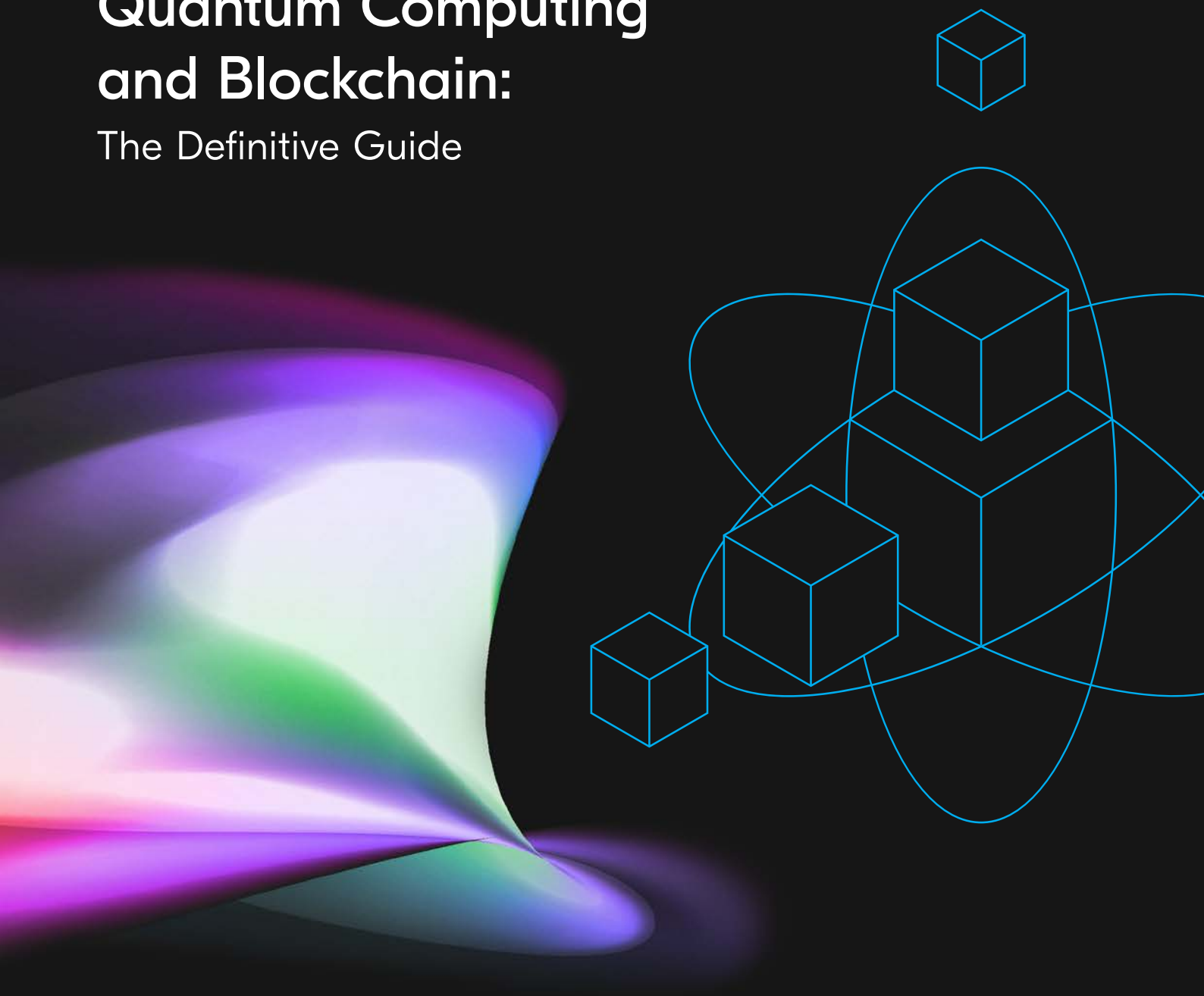
QAN

BLOCKCHAIN PLATFORM

Quantum Computing and Blockchain:

The Definitive Guide

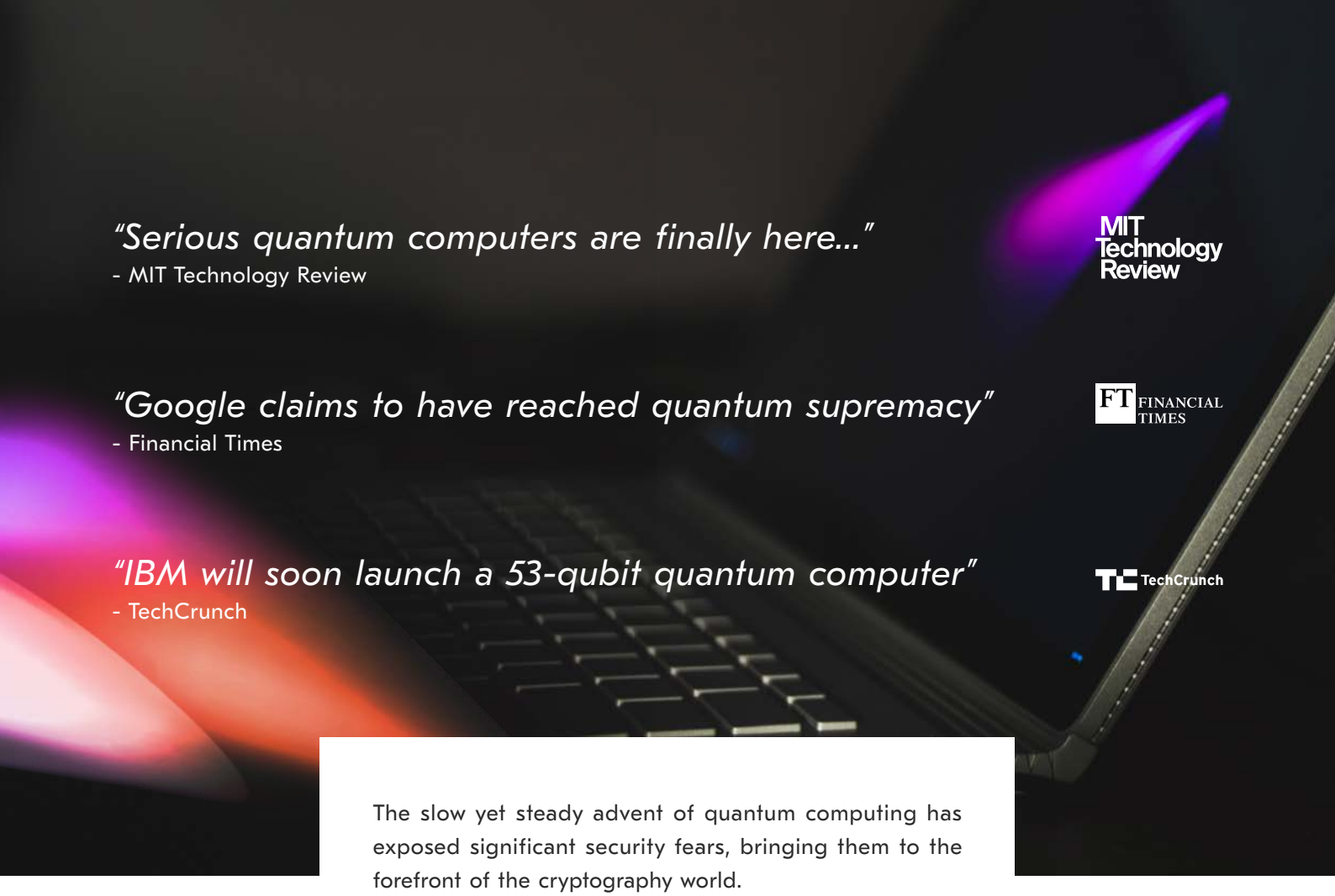


powered by

centrum circle

QANPLATFORM.COM

Contents List



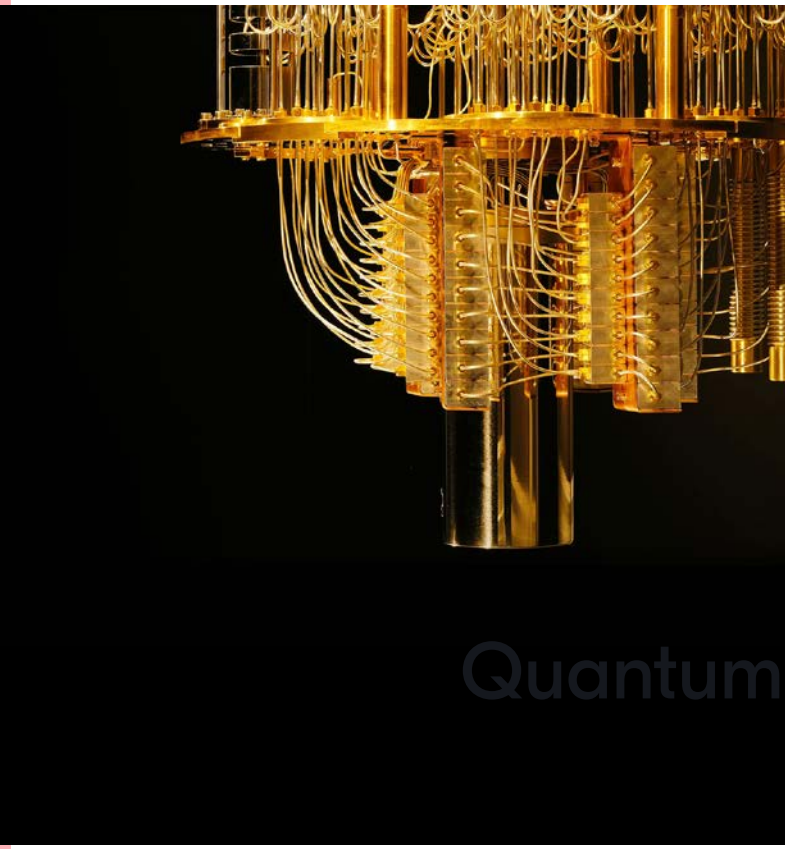
The slow yet steady advent of quantum computing has exposed significant security fears, bringing them to the forefront of the cryptography world.

Due to the fact that cryptography is an essential foundation of much of our lives as we know them, quantum computers pose a threat to a wide array of industries.

But do we really need to worry today?

You will learn in this ebook about *the problem, its origin, mechanisms,* and *implications* as well as the steps that are being taken to remedy the threat that quantum computers pose. Lastly, you will discover a quantum-resistant blockchain platform.

Let's dive right in.



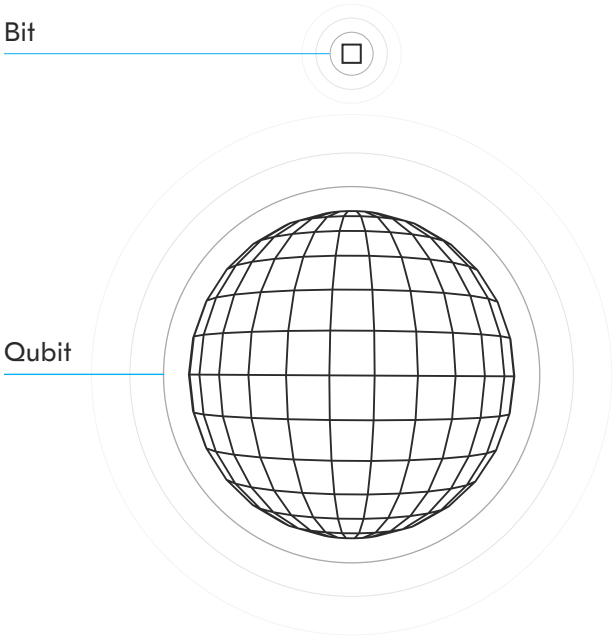
Quantum computer vs classic computer

To further understand the difference between quantum and classical computers, consider that classical computers, such as your PC, are binary in nature. In other terms, classical computers utilize bits in the form of transistors which can exist in either of two values — 0 or 1. Contrastingly, quantum Computers use Qubits which can either take a value of 0 or 1 or both simultaneously in a state of superposition.

Thus, theoretically speaking, quantum computers are capable of efficiently handling a much greater number of instructions per second than their classical counterparts. Data in a quantum computer is stored in qubits, where it can exist in more than one state, and because of this, there is an exponential increase in the millions of instructions per second (MIPS).

Data in quantum computers is denoted in Qubits, which are similar to normal bits, except that they can take on more than one value, sometimes many, simultaneously.
Furthermore, due to the fact that information in quantum computers is not stored or processed in a binary manner, the machine is able to "think" different "thoughts" at the same time. This simultaneous consideration of varying end states from the same set of particles/variables/data allows quantum computers to have much faster processing capabilities.

Based on their impressive processing capabilities, quantum computers represent a risk for cryptography as we know it. Robert Schoelkopf, a Yale professor and founder of a company called Quantum Circuits, reiterates the danger posed by the emergence of quantum computing.



Schoelkopf says:

"If you had 50 or 100 qubits and they really worked well enough, and were fully error-corrected—you could do unfathomable calculations that can't be replicated on any classical machine, now or ever. The flip side to quantum computing is that there are exponential ways for it to go wrong."

Robert Schoelkopf | Picture via Weforum

What is quantum speedup?
Grover's algorithm when used in combination with a quantum computer, could find a specific name in a phone book with 100 million names in just 10,000 operations. A classical search algorithm, employing its typical mechanisms to compute the data, which would simply mean looking through all the names, would need 50 million operations - on average - to find the same name.

Unfortunately, the quality of quantum computers which makes them so advantageous in certain industries is ultimately what makes them so dangerous for cryptography. Quantum speedup means that quantum computers can break cryptographic algorithms at a much faster rate than classical machines and supercomputers.

Just as Grover's algorithm is able to achieve impressive results in the search for specific data in large data sets, there is a quantum algorithm that allows the user to decipher the prime integers of a number (N) in polynomial time. Created in 1994, the algorithm is called Shor's algorithm and is named after its creator, the mathematician Peter Shor.

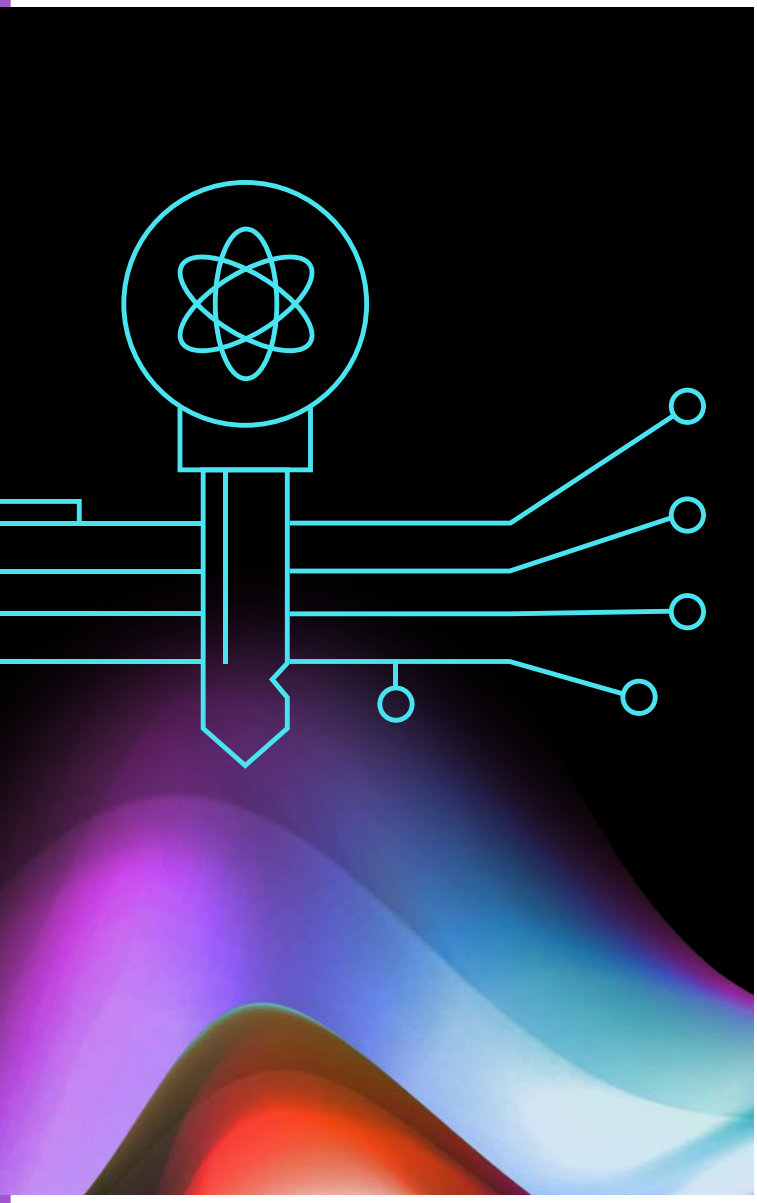
Employing Shor's algorithm, it is relatively simple to find the prime factors of very large numbers. This is a significant threat to cryptography as we know it because the generally accepted standards currently involve the use of PKC, which is based on this mathematical problem.

As determined earlier, most public-key cryptosystems are of the asynchronous persuasion. This means that there is a public and private key. Employing Shor's algorithm, quantum computers can wreak havoc on all PKC cryptosystems because if there is knowledge of one fact concerning an integer, such as a public key, then the machines can uncover the prime factorization thereby breaking the code and decrypting the data.

"Unfortunately, through a combination of the public key, generally made available as part of the RSA cryptosystems, and Shor's algorithm, quantum computers are theoretically able to break RSA encryption."

3.2 Post Quantum Algorithms

What is post-quantum cryptography?
Post-quantum cryptography is defined as the study of cryptosystems which can be executed on a classical computer or a super computer but remain secure even when running on a quantum computer. The goal is not to make classical computers obsolete by creating algorithms that are not backward compatible. This would be infeasible and lead to a crisis in and of itself.



Instead, as **NIST** explains:

"The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks."

To this end, NIST reviewed the submissions and published those that are the most promising in terms of creating a quantum-resistant future.

NIST identified the proposals with the greatest promise as those whose cryptosystems are based on:

- Lattices,
- Isogenies,
- Codes,
- Hash functions,
- Multivariate systems.