Today we live in an online world, constantly sharing information with each other. Among the information being shared are our transactions through our banks, messages to loved ones and top-secret government information. Close to all this information is being encrypted by public-key encryptions, most widely used is the RSA-algorithm. The security and strength of the RSA-algorithm lies in the assumption that multiplying large prime (large being integers with upwards of 2000+ digits) numbers together is an easy task whilst doing the opposite, factoring large numbers, is a fundamentally hard problem to solve, even for the most powerful supercomputers.

This assumption was challenged by Peter Shor who in 1994 published a paper containing an algorithm that could theoretically factor said large numbers using quantum computers. Quantum computers are computers that take use of quantum mechanical phenomena such as superposition and entanglement to exponentially get more powerful to the point where they can solve problems that otherwise would be impossible to solve on classical computers in a realistic timeframe. As more and more research has been done in the field of quantum computing, the looming threat of RSA one day being broken has become a near certainty which has caused governments and companies to invest billions in preparing for a post-quantum world.

Shor's algorithm demonstrates how quantum mechanics can be used to solve problems that would have otherwise been deemed impossible. And the possible applications go way beyond cryptography and include a new quantum internet, the possibility of simulating molecules at quantum level to help us build new materials and drugs, and much more.

We are today in the beginning of a transition into a new era of computing, cryptography, and the internet. And that era being the one of quantum.