# Post Quantum Cryptography: Should You Panic?

In September 2024, Chinese researchers were [reportedly able to break the RSA algorithm using a quantum computer](https://www.kaspersky.com/blog/quantum-cryptography-2024-hype/52884/). While that turned out to be a lie, quantum computers are a real threat to society, and already, many companies are working to protect the future of their cryptography.

Quantum computers are coming, and whether or not you work in privacy or blockchain, you should be concerned. But don’t panic, as solutions are already underway. Read on to learn more about post-quantum cryptography.

## What is Post Quantum Cryptography?

First and foremost, if you have questions about post-quantum computers, please read our sister article about the [threats of quantum computers to cryptocurrency,](https://www.mintdice.com/blog/are-quantum-computers-a-threat-to-crypto) published in October 2024, to give you a basic knowledge of the topic.

Back to the current topic at hand, the 2024 Chinese incident opened the world’s eyes to the necessity of implementing [post-quantum cryptography](https://csrc.nist.gov/projects/post-quantum-cryptography) (PQC) sooner rather than later. Although this may be the first time you are hearing about this topic, know that many large companies have already begun to consider the future, and several countries have already established regulations to govern the adoption of PQC.

PQC already exists, though it is still in the research stage, with post-doc research being completed by the likes of [Sonia Duc](https://www.linkedin.com/in/bogos-sonia/) and [Krijn Reijnders](https://www.rsaconference.com/experts/krijn-reijnders) in the EU, we are confident that humans will be able to adopt to this change—just as we have every other technological crisis in history. Y2K didn’t end us, and [quantum computers won’t either](https://www.cloudflare.com/learning/ssl/quantum/what-is-post-quantum-cryptography/).

[Current cryptography](https://www.mintdice.com/blog/the-history-of-cryptography) comes down to two basic algorithms, [Shor’s Algorithm](https://www.youtube.com/watch?v=dONacVnW1Ng) and [Grover’s Algorithm](https://quantum.cloud.ibm.com/learning/courses/fundamentals-of-quantum-algorithms/grover-algorithm/introduction). We are pleased to report that a post-quantum patch is already available for Grover’s Algorithm, which means researchers aren’t necessarily concerned about the future of this algorithm. They are, however, concerned about Shor’s Algorithm, which is still being explored to find a post-quantum solution that is [both efficient and effective](https://www.reddit.com/r/QuantumComputing/comments/1blpt3u/why_isnt_postquantum_encryption_more_widely/).

Basically, it comes down to this: to protect the future of cryptography, it is likely that the use of Shor’s algorithm for encryption will need to cease, and mathematicians are working to find a stronger algorithm to replace it with.

## When Will Post-Quantum Cryptography Be Required?

Currently, the quantum computers in the experimental stage are unable to produce results that would have us concerned—mostly because it is extremely difficult to keep qbits active and cooled. But this will change.

Which brings us to the next issue in the PQC world: researchers don’t know exactly when it will happen. They believe it is likely to occur as early as 2030 (though it could happen a bit earlier) and most likely to occur before 2040. This means the world only has about 10-12 years to prepare for quantum computers. As such, most countries have specified that they will [switch to PQC before 2035](https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards).

## Will Post-Quantum Cryptography Solve All Issues?

In short, while the above paragraphs may provide you with some relief from your fears of quantum computers, [Sonia Duc](https://www.linkedin.com/in/bogos-sonia/) pointed out that our fears may need to go far beyond that.

Criminals know that quantum computers are coming, and some may have adopted the “harvest now, decrypt later” tactic, meaning they harvest valuable encrypted data now, storing it for decryption when quantum computers crack current algorithms. Companies that store legacy data, such as those in the healthcare and financial industries, are the ones most affected by this issue.

Therefore, most countries have gone as far as to specify that this data should be protected first, and, unsurprisingly, that has led to many large companies already working to adapt PQC in 2025. Additionally, organizations like NIST have already established standards for PQC in preparation for rapid adoption in the coming years.

We would also like to note that there are many ways to adopt PQC, including hybrid models, which would wrap data encrypted by pre-quantum cryptography with the algorithms of PQC.

## Post Quantum Cryptography and Blockchain

One of the most common questions we get is how post-quantum cryptography will affect blockchain, and unfortunately, this is one of the industries that will be hit the hardest.

In our previous discussion on the subject, we mentioned that unmanned blockchains like Bitcoin will suffer the most—especially with the [SHA-256 algorithm](https://nordvpn.com/blog/sha-256/?srsltid=AfmBOoqqMRNqw024ZFYW1RaQFyJ41QHbzZCmNvvdUxkq1BKS2N8s2IKl) cracked. While this will be good news for those desperate to know who [Satoshi Nakamoto](https://www.mintdice.com/blog/who-is-satoshi-nakamoto) is, it will also expose every Bitcoin transaction ever, and we aren’t sure the blockchain will survive.

As of the writing of this article in August 2025, the only blockchain we are certain will survive quantum computers is Ethereum. [Vitalik Buterin](https://www.binance.com/en/square/post/28725089740225) is already aware of the coming storm, and is currently [taking steps to advance the Ethereum blockchain](https://ethereum.org/en/roadmap/future-proofing/) so that it will be protected.

We can’t say the same thing about any other blockchain. While we do believe those outside of the cryptocurrency world may be able to survive (such as companies in the public sector that utilize blockchain for supply chain), we make no promises.

## Companies Currently Working to Implement Post-Quantum Cryptography

As we mentioned above, many companies are currently working to ensure they are protected on the day when post-quantum computing becomes a reality. They are as follows:

* Signal
* iMessaging
* Cloud Flare
* Google Chrome
* AWS
* OpenSSH
* PQShield
* Ethereum

It is worth noting that these are all large companies, which are responsible for their own PQC. Many smaller and medium-sized companies that utilize vendors like AWS will be protected simply because they do not manage these aspects of their business in-house.

Overall, thinking of a world with quantum computers as the norm is terrifying. But whether or not you are afraid, it is a reality, and it is coming. Sure, we likely have 10 years before quantum computers hack the best cryptography algorithms, but they may be able to break them sooner. It’s time to invest in post-quantum cryptography and switch to using the businesses that are preparing for this date, no matter what industry you are in. Unfortunately, we can almost guarantee that some companies won’t adapt in time, and ultimately, their customers and brand image will suffer.