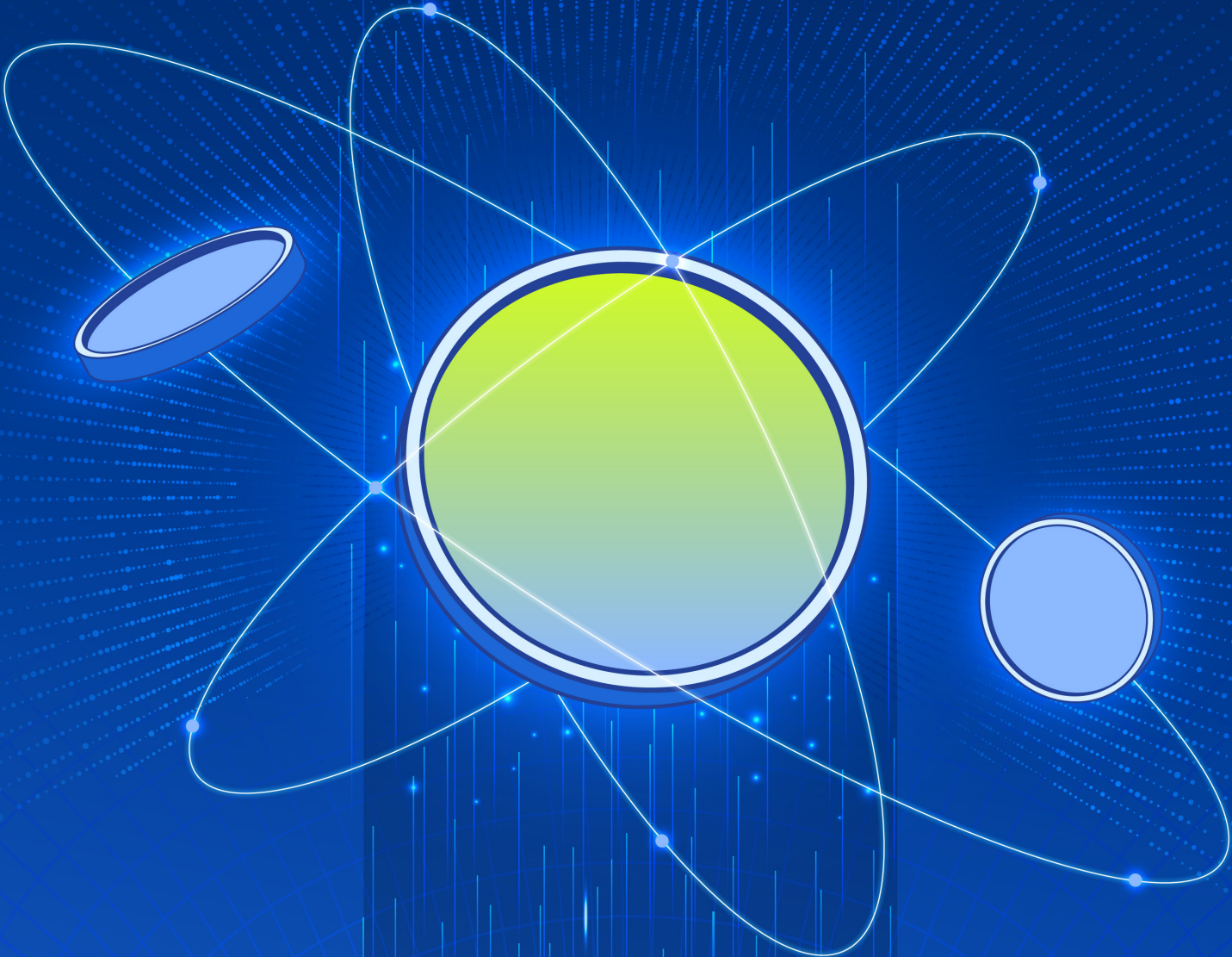


A central graphic depicting a quantum system. It features a large, glowing yellow-green sphere with a blue outline, surrounded by three smaller blue spheres. These are connected by white, elliptical orbits. The background is a deep blue with a grid of white dots and lines, suggesting a digital or quantum space.

# **QUANTUM COMPUTING AND CRYPTOCURRENCIES**

Bridging technical expertise  
and decision-making

# Table of Contents

## **3 | Executive summary**

- Key findings — 3
- Primary risk — 4
- Mitigation strategies — 4
- Recommendations — 4
- Conclusion — 4

## **5 | I. Introduction**

## **6 | II. Quantum computing**

- a. Principles behind quantum computing — 6
- b. Status of quantum computers — 8
- c. Cryptographically-relevant quantum capabilities — 10

## **12 | III. Cryptocurrencies and their security foundations**

- a. Proof-of-work, proof-of-stake and blockchain integrity — 12
- b. Wallet security and public-key cryptography — 13
- c. Decentralised governance and migration challenges — 14

## **15 | IV. Moving toward a safer ecosystem**

- a. Incremental upgrades for quantum resistance — 15
- b. Adoption of post-quantum standards — 16
- c. Using quantum technology to secure the blockchain — 18
- d. The challenge of the transition to PQC — 19

## **20 | V. Conclusion**

## **21 | VI. Policy guidelines**

# Executive summary

This report by Europol's European Cybercrime Centre (EC3) evaluates the potential implications of quantum computing on the cryptocurrency landscape. The report delivers an in-depth technical analysis that pinpoints genuine risks, recommends mitigation strategies, and addresses misconceptions that could influence the future of cryptocurrencies.

The report builds on Europol's existing work on quantum technologies, including *The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement*<sup>1</sup>, the *Quantum Safe Financial Forum – A call to action*<sup>2</sup>, and the *joint report on Prioritising Post-Quantum Cryptography Migration in Financial Services*<sup>3</sup>. These series of publications focus on raising awareness, supporting preparedness, and promoting the transition towards post-quantum cryptography.

## Key findings

---

**01.** Quantum computing poses **a credible threat to current public-key cryptography**, potentially impacting the security of digital assets.

---

**02.** The blockchain's core integrity, secured by cryptographic hash functions, remains largely resistant to quantum attacks. **The primary risk lies in the vulnerability of cryptocurrency wallets** that rely on public-key cryptography.

---

**03. Proactive adaptation**, rather than systemic collapse, is the most likely outcome. Cryptocurrencies can evolve through incremental upgrades, adoption of post-quantum cryptography (PQC) and exploration of quantum-enhanced security measures.

---

---

1 <https://www.europol.europa.eu/publications-events/publications/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement>

2 <https://www.europol.europa.eu/publications-events/publications/quantum-safe-financial-forum-call-to-action>

3 <https://www.europol.europa.eu/media-press/newsroom/news/joint-report-outlines-practical-approach-to-prioritising-post-quantum-cryptography-migration-in-financial-services>

## Primary risk

Cryptocurrency wallets, which utilise public-key cryptography to authorise transactions and control funds, are the primary point of exposure to quantum threats. Once sufficiently powerful quantum computers are developed, these keys could be compromised, leading to unauthorised access and potential loss of funds. However, solutions already exist.

## Mitigation strategies

- ▶ **Incremental upgrades:** implement account abstraction and multi-signature schemes to reduce reliance on single public keys and enhance wallet security.
- ▶ **Post-quantum cryptography (PQC) adoption:** transition to NIST-standardised PQC algorithms (e.g. CRYSTALS-Kyber, CRYSTALS-Dilithium) to replace vulnerable cryptographic schemes.
- ▶ **Quantum-enhanced security:** explore the potential of quantum key distribution (QKD) and other quantum technologies to further strengthen blockchain security, though scalability remains a challenge.

## Recommendations

- ▶ **Decision makers and regulators:** establish clear guidelines for PQC adoption and incentivise industry collaboration on quantum-resistant solutions.
- ▶ **Blockchain projects:** prioritise the integration of PQC algorithms into core protocols and provide resources for wallet providers to implement these changes.
- ▶ **Wallet providers:** begin testing and deploying PQC-enabled wallets, and educate users about the risks and benefits of quantum-resistant cryptography.
- ▶ **Users:** stay informed about the evolving quantum threat and proactively migrate funds to quantum-resistant wallets as they become available.

## Conclusion

Cryptocurrencies will not collapse due to quantum computing, but their long-term security requires proactive defence. By embracing innovation, fostering collaboration and prioritising a phased transition to quantum-resistant cryptography, the cryptocurrency ecosystem can build a safer, more resilient and trustworthy future. The time to act is now, to lay the foundation for a quantum-resistant digital economy.

# I. Introduction

Cryptocurrencies have rapidly evolved from a niche technological experiment to a globally recognised asset class and a platform for decentralised applications. This ascent has been accompanied by increasing scrutiny, not only from financial regulators and traditional institutions, but also from a growing chorus of commentators highlighting potential vulnerabilities. Among these concerns, the threat posed by the development of quantum computing has gained significant traction, frequently appearing in headlines and fuelling narratives of impending obsolescence for digital currencies. While quantum technologies promise transformative advancements across diverse sectors – from accelerating drug discovery and materials science to revolutionising financial modelling – they also introduce a fundamental challenge to the cryptographic foundations upon which modern digital security, and cryptocurrencies specifically, are built.

The core of this concern lies in the potential for quantum computers to break widely used public-key encryption algorithms. These algorithms, such as Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC), underpin the security of countless digital transactions, communications and data storage systems. However, the advent of sufficiently powerful quantum computers, leveraging algorithms like Shor’s, could render these algorithms ineffective, potentially exposing sensitive data and undermining trust in digital infrastructure. This has led to widespread speculation about the future of cryptocurrencies, with some predicting their complete collapse in the face of quantum attacks.

However, such a conclusion is overly simplistic. Cryptocurrencies are not solely reliant on public-key cryptography. They also employ symmetric cryptography and, crucially, cryptographic hash functions, which exhibit a different security profile. While public-key schemes are vulnerable to quantum algorithms, hash functions, used extensively in blockchain integrity mechanisms such as proof-of-work and proof-of-stake, are considered more resilient, although not entirely immune, to quantum attacks. Therefore, the threat is not necessarily the complete eradication of cryptocurrencies, but

rather a targeted vulnerability in the ownership and control of digital assets – specifically, the security of cryptocurrency wallets.

This report undertakes a comprehensive analysis of the impact of quantum computing on cryptocurrencies. We will clearly delineate the extent of the quantum threat to cryptography, detailing the algorithms at risk and the timeline for potential breakthroughs. We will then examine how cryptocurrencies utilise cryptography, highlighting the interplay between vulnerable and resilient cryptographic primitives. Crucially, we will propose a range of mitigation strategies, from incremental upgrades to the adoption of post-quantum cryptographic standards, and explore the potential for leveraging quantum technologies to enhance blockchain security. Finally, we will present a reasoned conclusion based on our analysis and offer actionable recommendations to policymakers, industry stakeholders and users, with a view to facilitating a proactive and secure transition to a quantum-resistant future for cryptocurrencies.

This report aims to move beyond sensationalism and provide a nuanced, evidence-based assessment of the challenges and opportunities presented by the convergence of quantum computing and blockchain technologies.

## II. Quantum computing

Quantum computing was born in the early 1980s<sup>4</sup>. It is expected to have as much impact, if not more, as previous technological developments based on quantum mechanics (such as the transistor in 1947, the atomic clock in 1949 or the laser in the mid-1950s). However, these new developments could pose a threat, if they are not accompanied by the corresponding mitigation.

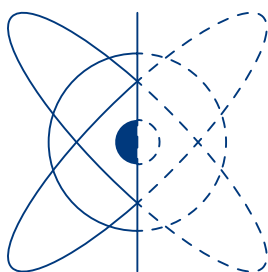
To understand and demystify the threat that quantum computing poses to cryptocurrencies, it is crucial to understand the basic principles of quantum computing, its current state of development and the impact it will have on the technologies on which cryptocurrencies are based.

### a. Principles behind quantum computing

Quantum computing<sup>5</sup> is an emerging class of computing technology that operates on fundamentally different principles from classical computers. While classical computers process information using bits that are either 0 or 1, quantum computers use quantum bits, also called *qubits*, which can represent both states (0 and 1) simultaneously according to the quantum mechanical phenomena known as **quantum superposition**.

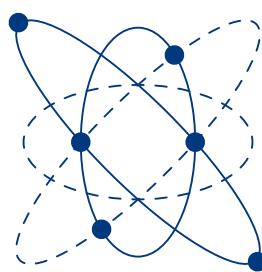
Similarly to the Schrödinger's cat thought experiment, those quantum particles convey both states simultaneously. However, measuring (observing) a qubit will make this superposition collapse to a single state (0 or 1), somehow converting the qubit to a regular bit.

*p. I*



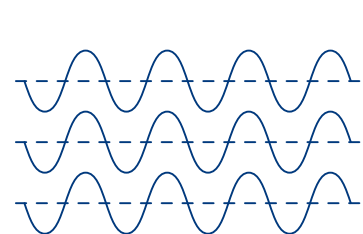
*quantum superposition*

*p. II*



*quantum entanglement*

*p. III*



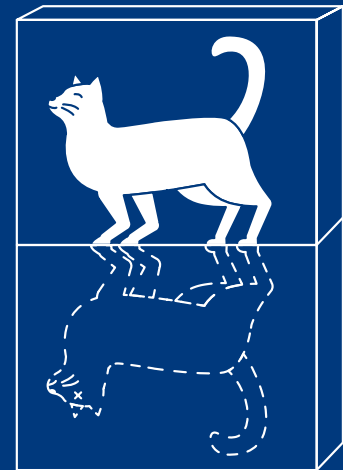
*quantum interference*

<sup>4</sup> Benioff, Paul, 'Quantum mechanical Hamiltonian models of Turing machines', Journal of Statistical Physics, 1982

<sup>5</sup> Ghose, Shohini (IBM), A beginner's guide to quantum computing – video recording of TEDWomen conference

**Schrödinger's cat** is a thought experiment devised in 1935. Imagine a cat sealed in a box with a radioactive atom, a Geiger counter, and a vial of poison. If the atom decays, the counter triggers and the poison is released, killing the cat. If it doesn't decay, the cat lives. According to quantum mechanics, before you open the box, the atom is in a superposition of decayed and not decayed – which implies the cat is both alive and dead at the same time.

Schrödinger invented this scenario to mock the idea, not to promote it. He wanted to show how absurd it is to apply quantum superposition to everyday objects like cats. Ironically, the thought experiment became one of the most famous illustrations of quantum theory, even though it was originally meant as a critique of its apparent irrelevance to the macroscopic world.



Another crucial quantum property in quantum computing is the property of **quantum entanglement**. Two or more entangled particles become linked in such a deep way that they act like a single system, even when they are far apart<sup>6</sup>. Entanglement lets qubits work together instead of separately, and measuring one particle instantly tells you something about the other one.

Quantum computers exploit superposition and entanglement to represent and manipulate a large space of possible states. However, these properties alone are not sufficient to achieve a quantum speedup. The crucial mechanism is **quantum interference**, through which a quantum algorithm is designed to amplify the probability of correct outcomes while suppressing incorrect ones during the computation.

When the system is finally measured, the quantum state collapses to a single outcome, ideally corresponding to the expected result. This process is inherently probabilistic; quantum algorithms must increase the likelihood of obtaining the correct answer, but do not guarantee it in a single run. Quantum superpositions cannot be

directly observed or 'read', which fundamentally limits how quantum computations can be used and interpreted.

In practical terms, this allows quantum computers to perform **certain** categories of calculations much more efficiently, sometimes with an exponential gain in complexity, than classical computers. It remains important to understand that such a gain is not universal, however, and only applies to specific algorithms. Nevertheless, unlike incremental improvements in classical computing, quantum computing represents a discontinuous technological shift. It introduces new computational capabilities rather than simply faster versions of existing ones.

<sup>6</sup> Horodecki, R., Horodecki, P., Horodecki, M., & Horodecki, K., 'Quantum entanglement', Reviews of Modern Physics, 81(2), 2009, pp. 865–942, <https://doi.org/10.1103/revmodphys.81.865>

## b. Status of quantum computers

The European Union and countries worldwide are investing heavily in quantum computing, supporting a wide range of technologies and infrastructures as listed in *Table 1* below. Through initiatives like the EU Quantum Technologies Flagship<sup>7</sup> and EuroHPC JU<sup>8</sup>, the European Union

has developed working prototypes, software tools and spin-offs, while also deploying early quantum systems across member states. These efforts aim to foster a sovereign, competitive quantum industry and expand the market for both hardware and software solutions.

| Technology platform | Superconducting | Ion Traps | Cold atoms | Photonics | Spin Qubits |
|---------------------|-----------------|-----------|------------|-----------|-------------|
| EU machines         | 17              | 6         | 8          | 5         | 3           |
| UK machines         | 4               | 6         | 0          | 5         | 2           |
| USA machines        | 26              | 7         | 4          | 2         | 0           |
| Canada machines     | 13              | 0         | 0          | 1         | 0           |
| China machines      | 1               | 0         | 0          | 1         | 3           |

*Table 1: Quantum computing and simulation suppliers landscape (source: Quantum Europe Strategy: Quantum Europe in a Changing World<sup>9</sup>)*

Quantum computers can be built using different technological approaches. There are many different ways to interact with, generate and manipulate subatomic particles, such as, using superconductive materials, laser beams and photonic circuits<sup>10</sup>. Maintaining these systems can be technically challenging and costly, though the specific requirements vary by platform. Superconducting qubits, for example, requires extremely low temperatures (close to absolute zero) to maintain coherence. Trapped-ion and neutral-atom qubits typically operate at room temperature or in slightly cool conditions, but require precise laser control and ultra-high vacuum systems. Photonic qubits can also function at ambient temperatures but demand sophisticated optical setups. In all cases, the delicate nature

of qubits makes quantum computing hardware significantly more difficult to build and maintain than classical systems, which constitutes a serious obstacle to quantum computers' calculations.

Notably, noise, both environmental and internal, represents a big challenge<sup>11</sup> because, regardless of the processors' power, it significantly multiplies computational error, therefore directly inhibiting the computer's operations. On one hand, because many computers operate at above-zero temperatures (to preserve quantum states), thermal radiation and other quantum phenomena affect qubits' calculations and lead to their degradation. On the other hand, error multiplication also derives from the nexus between physical

<sup>7</sup> [Quantum Flagship](#)

<sup>8</sup> [The European High Performance Computing Joint Undertaking \(EuroHPC JU\)](#)

<sup>9</sup> [COM\(2025\) 363 final - Quantum Europe Strategy: Quantum Europe in a Changing World](#)

<sup>10</sup> [Qubits, Institute for Quantum Computing, University of Waterloo](#)

<sup>11</sup> [Quantum computing is taking on its biggest challenge: noise](#), MIT Technology Review

and logical qubits. Physical qubits are the raw, error-prone units of a quantum computer (such as ions or superconducting circuits), while logical qubits are error-corrected, reliable units formed by combining multiple physical qubits. In other words, logical qubits are used for running algorithms, while extra physical qubits are dedicated to error correction and redundancy. As we add more logical qubits, the number of possible errors grows faster than the number of qubits themselves. Each logical qubit requires many physical qubits and extra operations for error correction, meaning that the total number of errors can grow in a non-linear way<sup>12</sup>.

Quantum error correction is a critical milestone for any company or start-up developing a quantum computer. In 2021, Google announced its goal of building a useful, error-corrected quantum computer within the decade<sup>13</sup>, while IBM's

Quantum Roadmap sets a target of a fault-tolerant quantum computer by 2029. However, the timeline for when quantum computers will be powerful enough to solve currently intractable problems remains uncertain. Although recent research claims to have achieved quantum supremacy<sup>14</sup>, the practical relevance of the problems solved is still debated. The 2025 Quantum Threat Timeline Report<sup>15</sup> surveyed 32 global experts from academia and industry. *Figure 1* summarises their expectations as regards when a quantum computer could break RSA-2048, a widely used cryptosystem, within a reasonable timeframe (24 hours).

Thus, quantum computers are likely to become a reality in the medium to long term. It is therefore critical to assess the risks they pose to society and, in the context of this document, to the cryptocurrency ecosystem in particular.

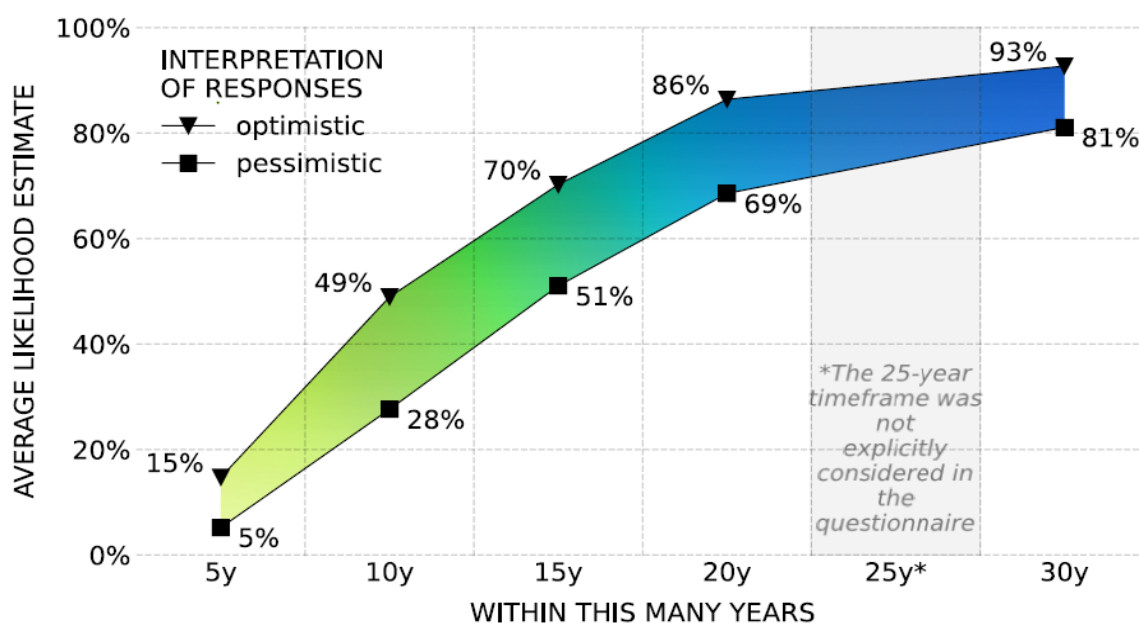


Figure 1: 2025 Opinion-based estimates of the likelihood of a digital quantum computer able to break RSA-2048 in 24 hours, as function of time. (source: Quantum Threat Timeline Report 2025 - EvolutionQ, GRI (4))

<sup>12</sup> Google Quantum AI, 'Suppressing quantum errors by scaling a surface code logical qubit', Nature 614, 2023, pp. 676–681, <https://doi.org/10.1038/s41586-022-05434-1>

<sup>13</sup> Erik Lucero, 'Unveiling our new Quantum AI campus', Google AI Blog, 18 May 2021, <https://blog.google/technology/ai/unveiling-our-new-quantum-ai-campus/>

<sup>14</sup> Quantum supremacy refers to the point at which a quantum computer can solve a problem that is practically impossible for classical computers to solve, even with extensive resources. It demonstrates the quantum computer's ability to outperform classical systems in specific tasks.

<sup>15</sup> [Quantum Threat Timeline Report 2025](#), Global Risk Institute

## c. Cryptographically-relevant quantum capabilities

Quantum technologies already have a significant impact on everyday life<sup>16</sup>. Well-known applications of quantum mechanics include semiconductor electronics, laser technology and magnetic resonance imaging (MRI). Beyond these established uses, ongoing progress in areas such as quantum sensing, quantum optimisation and quantum communication<sup>17</sup> is expected to enable a wide range of new technological capabilities.

This report focuses on cryptocurrencies and therefore restricts its scope to quantum technologies that are relevant to this context. In particular, it examines the potential impact of quantum computing on cryptographic algorithms that underpin the security of modern cryptocurrencies. There exist today two important algorithms with a potential concrete impact on current standards cryptography: Shor's and Grover's algorithms.

### SHOR'S ALGORITHM

Shor's algorithm<sup>18</sup> is widely regarded as the most significant quantum algorithm in the context of cryptography. It enables the efficient factorisation of large integers and the computation of discrete logarithms. Those problems are believed to be computationally unpractical for classical computers. Most of the classic public-key cryptographic systems, including RSA, Diffie-Hellman and elliptic curve cryptography, rely directly on the difficulty of these problems to ensure our modern digital-security. These systems are widely used today to secure web communications (TLS), software updates, digital identities and blockchain-based signature schemes.

The existence of Shor's algorithm implies that a sufficiently powerful and fault-tolerant quantum computer would be able to break these cryptographic schemes in polynomial time. In practical terms, this would allow an attacker to derive private keys from public information, enabling the forging of digital signatures or the decryption of previously secure communications. Although such quantum computers do not yet exist, this potential capability represents a fundamental threat to current public-key infrastructures and is the main driver behind the development, standardisation and transition to post-quantum cryptographic standards. Indeed, current data may already be at risk according to Mosca's inequality theorem<sup>19</sup>, which warns that data encrypted today could be decrypted in the future, threatening potential long-term confidentiality requirements.

<sup>16</sup> Scholten, T. L., et al., 'Assessing the Benefits and Risks of Quantum Computers', arXiv preprint, 2024, <https://arxiv.org/abs/2401.16317>

<sup>17</sup> Europol, 'The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement', Europol Innovation Lab Observatory Report, Publications Office of the European Union, 2023, <https://www.europol.europa.eu/publications-events/publications/second-quantum-revolution-impact-of-quantum-computing-and-quantum-technologies-law-enforcement>

<sup>18</sup> Shor, P. W., 'Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer', SIAM Journal on Computing, Vol. 26(5), 1997, pp. 1484–1509. <https://doi.org/10.1137/s0097539795293172>

<sup>19</sup> Michele Mosca, 'Cybersecurity in a quantum world: will we be ready?', <https://www.youtube.com/watch?v=VXh6xLrP7ys>

## GROVER'S ALGORITHM

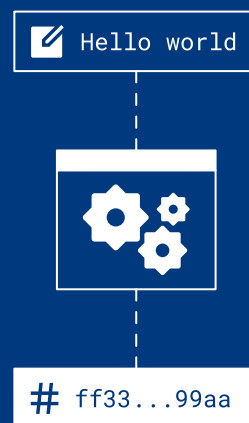
In contrast, Grover's algorithm<sup>20</sup> affects cryptography in a more limited but still relevant way. It provides a quadratic speedup for unstructured search problems, including brute-force attacks against symmetric encryption schemes and cryptographic hash functions.

These primitives are commonly used to protect stored data, secure communications channels and ensure data integrity, for example through encryption standards such as AES or hash functions used in password storage and blockchain mining.

A **cryptographic hash** function is a mathematical function that takes an input of arbitrary size (such as a file, a message, or a transaction) and produces a fixed-size output called a hash or digest. This output appears random, but it is completely determined by the input: the same input will always produce the same hash.

Hash functions are designed to be **one-way**: given a hash, it is computationally infeasible to recover the original input. They are also **collision-resistant**, meaning it is extremely difficult to find two different inputs that generate the same hash. These properties make hash functions useful for verifying data integrity and securing digital systems.

In cryptocurrencies, hash functions are fundamental. They are used to identify transactions and blocks, to link blocks together in a blockchain and to support consensus mechanisms such as proof-of-work. The security of these systems relies on the assumption that hashes cannot be predicted, reversed or efficiently manipulated.



Rather than completely breaking these systems, Grover's algorithm effectively reduces their security level. In practice, its impact can be mitigated by increasing key and hash sizes, for instance by moving from 128-bit to 256-bit keys. As a result, symmetric cryptography is generally considered more resilient to quantum computing than public-key cryptography, provided that the appropriate parameter choices are adopted.

Beyond these specific algorithms, quantum computing may also enhance general cryptanalytic capabilities. Improved search and optimisation techniques could facilitate the analysis of cryptographic constructions, including the new post-quantum cryptographic standards, or lower the cost of certain attacks. In the context of cryptocurrencies, where cryptography underpins ownership, transaction validation and consensus mechanisms, these developments raise important questions about long-term security and trust, and naturally motivate a closer examination of how quantum computing may affect cryptocurrency systems.

<sup>20</sup> Grover, L. K., 'A fast quantum mechanical algorithm for database search', STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing, 1996, <https://doi.org/10.1145/237814.237866>

### III. Cryptocurrencies and their security foundations

Cryptocurrencies are often perceived primarily as financial instruments or investment assets. While this is partially true, at their core they are cryptographic systems designed to provide **secure, decentralised** and **verifiable transactions without relying on traditional central authorities**. The security and reliability of these systems depend on mathematical and cryptographic principles, rather than institutional oversight. As a result, any shift in the underlying assumptions of cryptography, as discussed in the previous section, has the potential to impact cryptocurrencies in fundamental ways<sup>21</sup>. Before proceeding to a systematic review of the associated risks and countermeasures, it is useful to provide a brief reminder of the core principles underlying cryptocurrency systems.

Unlike traditional financial systems, where trust is placed in institutions, cryptocurrencies derive trust from **mathematical guarantees**. Transactions are validated through consensus mechanisms and recorded in a public ledger, known as a blockchain. The blockchain ensures that transactions cannot be altered once confirmed, providing transparency and security in a decentralised manner.

#### a. Proof-of-work, proof-of-stake and blockchain integrity

Cryptocurrencies rely on different consensus mechanisms to validate transactions and secure the blockchain, the most common being **proof-of-work (PoW)** and **proof-of-stake (PoS)**.

In PoW systems, such as Bitcoin, miners compete to solve computational puzzles based on cryptographic hash functions. These puzzles require finding an input that produces a hash output meeting a certain condition, such as a number of leading zeros. Hash functions are easy to compute in one direction but extremely difficult to invert, ensuring that altering a block in the ledger would require infeasible amounts of computation. Importantly, the security of PoW

depends on this computational difficulty rather than on secrecy; it guarantees that tampering with past blocks is prohibitively expensive.

PoS systems, like Ethereum post-merge, use a different approach. Validators are chosen to propose and confirm blocks based on the amount of cryptocurrency they 'stake' as collateral. While PoS does not rely on computational puzzles for security, hash functions still play a critical role in linking blocks and maintaining the integrity of the blockchain. Every block contains a hash of the previous block, forming a chain that is computationally secure against alteration. Because these hash functions are

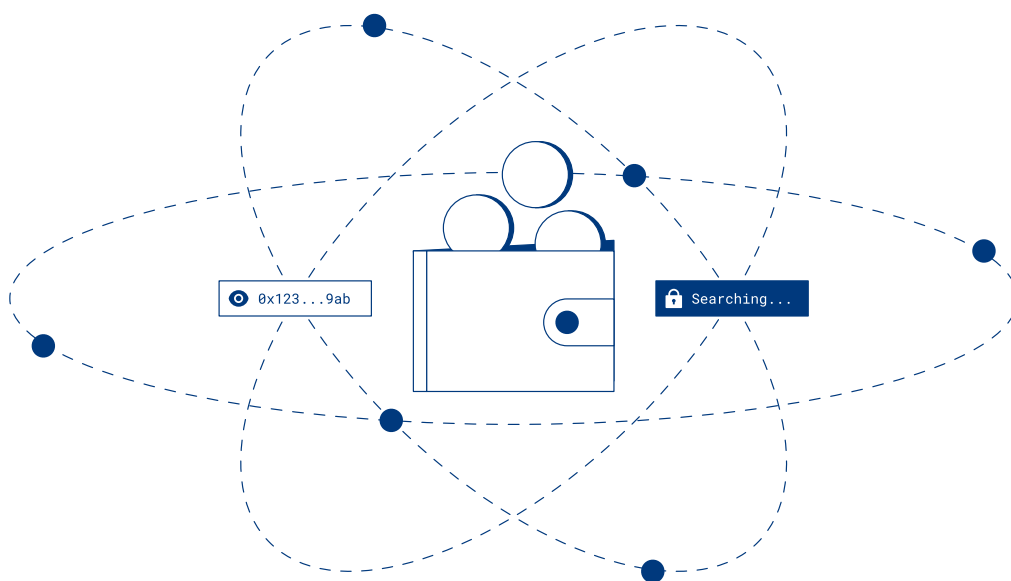
<sup>21</sup> Kappert, N., Karger, E., & Marko Kureljusic, 'Quantum Computing – The Impending End for the Blockchain?', Pacific Asia Conference on Information Systems (PACIS) 2021, Dubai, UAE, 114

resistant to inversion, the blockchain remains secure even under PoS, despite the absence of mining-based work.

In both PoW and PoS systems, hash functions are **largely quantum-safe**<sup>22</sup>. Quantum computers could accelerate certain search problems through algorithms such as Grover's algorithm, providing roughly a square-root speedup in finding hash preimages or collisions. For example, compromising a 256-bit hash would require on the order of  $2^{128}$  operations for a quantum computer, still astronomically high with foreseeable technology. This contrasts sharply with public-key

cryptography, which will be fully broken by quantum algorithms such as Shor's, and therefore requires separate mitigation strategies.

In short, the use of hash functions in both PoW and PoS ensures that the **integrity of the blockchain itself remains secure against quantum attacks**, making these mechanisms a robust foundation for decentralised networks, at least in the medium term. The primary quantum risk, as discussed in the next subsection, lies elsewhere: in the cryptography securing ownership and wallets.



## b. Wallet security and public-key cryptography

While the blockchain ledger itself is secured by hash functions and consensus mechanisms, the most sensitive part of a cryptocurrency system is the ownership of digital assets. This ownership is established and maintained through public-key cryptography, which functions similarly to a decentralised form of public-key infrastructure (PKI).

Every cryptocurrency wallet relies on a pair of cryptographic keys: a private key and a public key. The private key is kept secret and allows the owner

to authorise transactions, proving control over the associated funds. The public key, in contrast, can be shared openly and is used by the network to verify that any transaction claiming to spend funds from that wallet is valid. The cryptographic relationship between the private and public key ensures that the private key cannot be deduced through classical computation, thereby securing the wallet.

It is important to note that PKI in cryptocurrencies is not used to validate the blockchain itself. When

<sup>22</sup> Bernstein, D., Lange, T., 'Post-quantum cryptography', Nature, 549, 2017, pp. 188–194, <https://doi.org/10.1038/nature23461>

a miner discovers a new block in a proof-of-work system, or when a validator proposes a block in a proof-of-stake system, the network verifies the block's validity through hash functions and consensus rules, not through general-purpose digital signatures such as PKI. In PoW, the network only checks that the submitted proof-of-work meets the difficulty criteria, while in PoS, the protocol ensures the validator is eligible based on staked assets. Any signature included with a block is typically protocol-specific and serves to authenticate the proposer, not to secure funds.

The distinction is critical from a quantum perspective. While hash functions securing block integrity are currently quantum-resistant, the cryptographic keys used in wallets are vulnerable to sufficiently powerful quantum computers. Algorithms such as Shor's algorithm will derive a private key from a public key, allowing an attacker to spend funds without authorisation. This is exactly why **wallet security**, rather than blockchain integrity, is considered the **primary point of exposure to quantum threats**.

From a policy standpoint, this creates several important considerations. Unlike traditional financial systems, there is no central authority that can revoke compromised keys or enforce upgrades. Decentralised governance and long-lived addresses mean that vulnerabilities could persist for years if the migration to quantum-resistant cryptography is not carefully planned and coordinated. Moreover, the public visibility of blockchain keys enables adversaries to proactively target wallets, creating a latent risk of future attacks once quantum computers become capable, unless decisive action is taken to transition away from the status quo.

In summary, the **primary quantum risk** lies in **public-key cryptography** used by wallets, not the blockchain itself, which remains secure thanks to hash functions. The focus must therefore shift to practical mitigation: improving key management, educating users, upgrading protocols, and coordinating large-scale migration to quantum-resistant standards.

## c. Decentralised governance and migration challenges

Cryptocurrencies replicate many functions of traditional public key infrastructure (PKI) in a decentralised way, where identity verification and transaction authenticity are mathematically guaranteed rather than institutionally enforced. While this design enhances independence, it complicates critical upgrades, such as migration to quantum-resistant cryptography. In decentralised networks, upgrades require consensus among a global and diverse set of participants (e.g. miners, node operators, developers and users), making the implementation of new cryptographic standards slower and more complex than in centralised systems.

This governance challenge amplifies risk in ways that extend beyond quantum threats. For example, 51% attacks, which are where an entity gains majority control of a network's mining power, highlight the vulnerabilities inherent in decentralised **consensus** mechanisms. However, unlike quantum risks, these attacks are not exacerbated by advancements in quantum computing, as they rely on classical computational dominance and network dynamics. Even if quantum-safe algorithms exist, deploying them across millions of wallets and nodes remains a multi-year, resource-intensive effort, dependent on both technical adoption and community consensus.

## IV. Moving toward a safer ecosystem

Cryptocurrencies rely on a delicate balance of cryptographic assumptions and decentralised governance. While the blockchain's integrity is largely secure in the near term, the security of individual wallets and the trust in ownership of digital assets is vulnerable to potential advances in quantum computing. Understanding this distinction is essential. The primary risk is not systemic collapse but the exposure of funds and the loss of trust, which could have broader implications for market confidence and financial stability.

Nonetheless, while the development of quantum computers is already well under way, research into countermeasures has already put forward a set of solid viable options to protect current cryptographic standards, to upgrade and/or to integrate them with quantum technology. In the following section, we describe three subsets of possible countermeasures and discuss their viability.

### a. Incremental upgrades for quantum resistance

A first short-term solution to achieve quantum resistance focuses on structural and procedural improvements within existing blockchain frameworks, avoiding reliance on post-quantum cryptography (PQC). Instead, it leverages account abstraction, transaction validation methods and address management to reduce exposure to quantum threats.

A core challenge in blockchain security is the use of externally owned accounts (EOAs), traditional wallets controlled by private keys that directly expose public keys on-chain. Account abstraction, as proposed in Ethereum's ERC-4337 standard<sup>23</sup>, replaces EOAs with smart contract wallets, where transactions are executed by code rather than private keys. This design introduces a layer of indirection, reducing direct exposure of private keys, and enables integration with zero-knowledge proofs (e.g. ZK-STARKs<sup>24</sup>). ZK-STARKs validate transactions without revealing underlying key information, limiting the utility of harvested public keys for future decryption.

However, this raises the critical question about wallets whose public keys have already been exposed. For these, no cryptographic fix exists; once a public key is exposed, it remains permanently vulnerable to future quantum decryption. The only solution is pre-emptive migration. Users must transfer funds to new, unexposed wallets (e.g. smart contract wallets) before any quantum attack occurs. Exposed EOAs cannot be secured retroactively. They must be abandoned in favour of quantum-resistant alternatives.

Another layer of defence is systematic address rotation, where wallets automatically generate new public/private key pairs for each transaction. This forces adversaries to repeatedly re-target keys, rendering attacks impractical if keys are rotated faster than quantum computers can decrypt them. However, this method assumes quantum computers cannot achieve instant decryption, **a risk that grows with technological progress.**

<sup>23</sup> <https://docs.erc4337.io/core-standards/erc-4337.html>

<sup>24</sup> [What is ZK-Stark?](#), StarkWare

Additionally, frequent rotation could disrupt usability or strain network performance if not carefully managed.

In the event of a confirmed quantum attack, a hard fork could revert the blockchain to a pre-compromise state and disable vulnerable EOAs, mandating all transactions to use smart contract wallets with ZK-STARK validation. This is a reactive measure, however, and does not protect funds already spent from compromised wallets.

These conventional methods provide **immediate, practical mitigation**, but are not without limitations. Their effectiveness depends on **user adoption**. As migration from exposed wallets is not automatic, users must proactively transfer

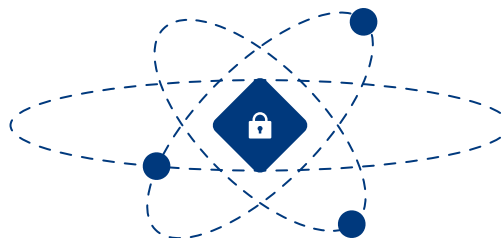
funds to new addresses. Governance also plays a critical role as hard forks and protocol upgrades require **community consensus**, which can be slow and contentious. Lastly, some of the techniques presented above would imply significant protocol changes in existing cryptocurrencies, such as Bitcoin, as they lack the infrastructure for account abstraction or smart contract wallets.

While these strategies **buy time**, they are **not foolproof**. If quantum computing advances faster than expected, **unmigrated funds in exposed wallets remain at risk**. These measures should therefore be viewed as **complementary to long-term solutions like post-quantum cryptography**, not as replacements.

## b. Adoption of post-quantum standards

The second approach directly confronts the quantum threat to foundational cryptographic standards such as the elliptic curve digital signature algorithm (ECDSA), which underpin not only the Bitcoin ecosystem but also global digital security infrastructure. With the recognition that this risk extends far beyond cryptocurrencies, threatening everything from financial systems to government communications, massive research and standardisation efforts have been mobilised to develop secure alternatives. Post-quantum cryptography (PQC) has emerged as the leading solution, providing algorithms designed to withstand quantum attacks while remaining compatible with classical hardware. By leveraging mathematically intractable problems, such as lattice-based cryptography, hash-based

signatures and code-based schemes, PQC offers a future-proof foundation for long-term security in both blockchain and traditional systems.



In 2024, the U.S. National Institute of Standards and Technology (NIST) finalised its first set of post-quantum cryptography (PQC) standards<sup>25</sup>, including CRYSTALS-Kyber<sup>26</sup> (key encapsulation) and CRYSTALS-Dilithium<sup>27</sup> (digital signatures), with a second standardisation phase<sup>28</sup> underway to diversify options beyond lattice-based solutions. This transition is not just a technical upgrade but a geopolitical priority, driven by coordinated

<sup>25</sup> [Announcing Issuance of Federal Information Processing Standards \(FIPS\) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice-Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard](#), NIST, 2024

<sup>26</sup> FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, NIST, 2024, <https://doi.org/10.6028/NIST.FIPS.203>

<sup>27</sup> FIPS 204, Module-Lattice-Based Digital Signature Standard, NIST, 2024, <https://doi.org/10.6028/NIST.FIPS.204>

<sup>28</sup> [NIST Announces 14 Candidates to Advance to the Second Round of the Additional Digital Signatures for the Post-Quantum Cryptography Standardization Process](#), NIST 2024

efforts across governments and standards bodies. In the European Union, the Coordinated

Implementation Roadmap for the Transition to Post-Quantum Cryptography<sup>29</sup> is backed by national cybersecurity agencies, such as:

- ▶ **Germany's BSI**<sup>30</sup> (Federal Office for Information Security), which has issued guidelines for PQC migration in critical infrastructure.
- ▶ **The Netherlands' AIVD** (General Intelligence and Security Service), together with the CWI and the TNO, have released a PQC migration handbook<sup>31</sup>.
- ▶ **France's ANSSI** (National Agency for the Security of Information Systems) has released its views on the post-quantum cryptography transition<sup>32</sup>.
- ▶ **The UK's NCSC** (National Cyber Security Centre), which, despite Brexit, aligns with EU efforts through its quantum-safe cryptography initiatives.

Beyond Europe, Japan's CRYPTREC<sup>33</sup> and Canada's CSE<sup>34</sup> (Communications Security Establishment) are also accelerating PQC adoption, while NATO's cybersecurity frameworks<sup>35</sup> now include quantum-resistant requirements for member states. These global mandates reflect a consensus: PQC is no longer optional; it is a necessity for national security and economic stability.

While Bitcoin and Ethereum have yet to transition, smaller projects such as the Quantum Resistant Ledger (QRL)<sup>36</sup> demonstrate that PQC is already viable. This was the first blockchain to fully implement XMSS (eXtended Merkle Signature Scheme), a hash-based, quantum-resistant signature algorithm, proving that PQC can be deployed at scale.

Despite these advancements, scalability and adoption remain challenging. For example, hash-based signatures (e.g. XMSS, Lamport) offer provable quantum resistance but suffer from large signature sizes (approximately 20KB instead of 72 bytes for the ECDSA), risking blockchain overload. Optimisations like Merkle tree-based key compression are under development to address this, but user migration and governance coordination pose even greater challenges.

The transition to PQC is a global imperative, not just a cryptocurrency issue. For blockchains, it demands wallet upgrades, consensus changes and community adoption, a complex but necessary evolution to avert catastrophic breaches. Before exploring the practical strategies and obstacles in achieving this transition, a third potential approach is described.

<sup>29</sup> [C\(2024\) 2393 final, COMMISSION RECOMMENDATION of 11.4.2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, European Commission](#)

<sup>30</sup> [Quantum Technologies and Quantum-Safe Cryptography](#), BSI

<sup>31</sup> [The PQC Migration Handbook](#), AIVD, CWI, TNO

<sup>32</sup> [ANSSI views on the Post-Quantum Cryptography transition](#), ANSSI, 2023

<sup>33</sup> [Cryptographic Technology Guidelines](#), Cryptrec

<sup>34</sup> [Preparing your organisation for the quantum threat to cryptography \(ITSAP.00.017\)](#)

<sup>35</sup> [Summary of NATO's Quantum Technologies Strategy](#)

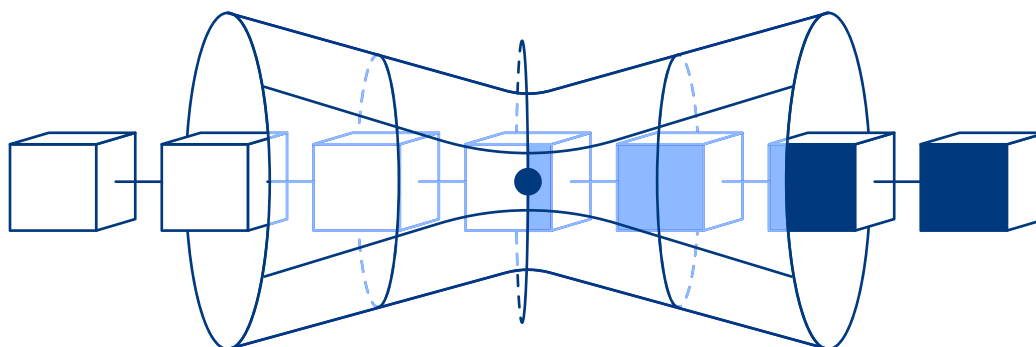
<sup>36</sup> <https://www.theqrl.org/>

## c. Using quantum technology to secure the blockchain

Countermeasures such as **quantum cryptography**, which uses principles of quantum mechanics to secure communications, can also leverage quantum technology itself. **Quantum key distribution (QKD)**<sup>37</sup>, for example, enables two parties to generate a shared secret key by transmitting photons through fibre-optic cables.

theorem<sup>40</sup> to associate coins with unique quantum states, but their 2GB storage capacity pales in comparison to Bitcoin's 300GB blockchain.

In the near to medium term, classical post-quantum cryptography (e.g. lattice-based algorithms) is far more feasible for securing



The sender encodes information using polarised filters, while the receiver uses beam splitters to detect photon states. Any eavesdropping attempt disrupts the quantum states, alerting both parties to interference. This makes QKD theoretically **unhackable** under ideal conditions.

However, **practical deployment faces significant challenges**. Current QKD systems are limited to short distances (~500 km) due to photon degradation, requiring expensive repeaters for longer ranges. Proposals like quantum blockchains (e.g. Allende et al., 2021<sup>38</sup>) or quantum cryptocurrencies (e.g. Jogenfors, 2019<sup>39</sup>) remain **experimental and unscalable**. For instance, quantum cryptocurrencies rely on the no-cloning

cryptocurrencies. While quantum-resistant technologies hold **long-term promise**, their current limitations, scalability, cost and infrastructure requirements make them impractical for widespread adoption today. The focus should remain on **transitioning to quantum-safe classical algorithms** and improving governance for large-scale upgrades.

<sup>37</sup> Ma, Lijun, M., & Alan, T., Xiao, 'High Speed Quantum Key Distribution Over Optical Fiber Network System', Journal of Research of the National Institute of Standards and Technology, Vol. 114(3), 2009, p. 149, <https://doi.org/10.6028/jres.114.010>

<sup>38</sup> Marcos Allende, Diego López León, Sergio Cerón, Antonio Leal, Adrián Pareja, Marcelo Da Silva, Alejandro Pardo, Duncan Jones, David Worrall, Ben Merriman, Jonathan Gilmore, Nick Kitchener, Salvador E. Venegas-Andraca, 'Quantum-resistance in blockchain networks', arXiv, 2021, <https://doi.org/10.48550/arXiv.2106.06640>

<sup>39</sup> J Jogenfors, 'Quantum bitcoin: an anonymous, distributed, and secure currency secured by the no-cloning theorem of quantum mechanics', IEEE international conference on blockchain and cryptocurrency (ICBC), 2019, <https://doi.org/10.1109/BLOC.2019.8751473>

<sup>40</sup> Wootters, W., Zurek, W., 'A single quantum cannot be cloned', Nature, Vol. 299, 1982, pp. 802–803, <https://doi.org/10.1038/299802a0>

## d. The challenge of the transition to PQC

The most critical challenge in post-quantum migration is not the development of quantum-resistant algorithms, as these already exist, but the execution of a global transition under tight constraints. While symmetric encryption (e.g. AES-256) can be fortified against quantum attacks through key-size adjustments, asymmetric systems, which are the foundation of digital signatures, secure communications and financial transactions, face immediate obsolescence once sufficiently powerful quantum computers arrive.

Unlike traditional IT upgrades, post-quantum cryptography (PQC) adoption demands simultaneous modification of infrastructure, which typically evolves incrementally. Some sectors face acute risks due to 'harvest now, decrypt later' attacks. However, the threat landscape differs by use case: while HNDL poses existential risks to long-term confidential data (e.g. classified communications or medical records), its impact on financial transactions is more nuanced. For payment systems, the real-time interception of transactions, not retrospective decryption, represents the most immediate quantum risk. This distinction slightly eases the time pressure for some use cases but does not eliminate the urgency to begin the transition.

Beyond technical hurdles, the transition faces profound governance and scalability obstacles. Bitcoin's 90% miner consensus requirement for significant protocol changes, historically a source of contention as seen during the 2015-2017 SegWit debates<sup>41</sup>, could delay or fragment adoption. Meanwhile, NIST-standardised PQC schemes introduce signature sizes 10 to 120 times larger than the ECDSA, threatening to overload block space, increase fees and slow confirmation times, issues exacerbated by Bitcoin's already strained throughput. Even interim solutions like Taproot<sup>42</sup>, which adopted

Schnorr signatures in 2021, offer no quantum resistance and remain adopted by less than 1% of unspent transaction outputs (UTXOs) in value, limiting their utility as a bridge.

Assuming that the risk is well understood and that a consensus should be obtained, the transition will still not be immediate. A first and immediate action is the responsibility of wallet owners as wallets must be updated to adopt the changes. Such a process implies not only a software update, but also potentially a hardware update if the hardware (wallet) becomes incompatible with the new consensus. On a different level, the UTXOs will also need to be updated in the blockchain. Each update will require a transaction registered in the blockchain, which will limit the availability of the block for normal transactions. As the block size is already limited, even more so with the potential adoption of larger signatures, this will inevitably have an impact on the transaction time. A recent study from Pont et al.<sup>43</sup> estimates the transition time of all UTXOs to be at least a cumulative continuous downtime of 76 days. It is obviously untenable to fully block any transaction for more than two months. Hence, the transition could be spread over time to maintain a decent level of availability (for example, spread over 300 days by dedicating only 25% of each block to the transition).

Not all UTXOs fall under the same risk category, and this depends on the way they are stored in the ledger<sup>44</sup>. In their new form, the transaction only exposes an ephemeral public key during a short period of time until the transaction is confirmed. A quantum computer powerful enough to derive a private key during this time window could steal the funds in parallel. This scenario, defined by Pont et al. as a 'just-in-time (JIT) quantum attack', underlines the need for a **complete migration** of the cryptocurrency ecosystem **before the advent of practical quantum computers**.

41 <https://medium.com/@brenmcma/understanding-segwit-and-the-bitcoin-scaling-debate-c9f7170e9e79>

42 [https://en.bitcoin.it/wiki/BIP\\_0341](https://en.bitcoin.it/wiki/BIP_0341)

43 Jamie J. Pont, Joseph J. Kearney, Jack Moyler, Carlos A. Perez-Delgado, Downtime Required for Bitcoin Quantum-Safety, October 2024, <https://arxiv.org/pdf/2410.16965v1>

44 [Will Quantum Computing Break Bitcoin?](#) River Learn

## V. Conclusion

The transition to post-quantum cryptography is not just a challenge for cryptocurrencies; it is a **historic opportunity to strengthen their security, resilience and user trust**. Unlike traditional financial systems, where migrations can unfold over years under centralised control, decentralised networks like Bitcoin have the chance to demonstrate that trustless systems can **proactively and collaboratively** evolve to rise to the most advanced technological challenges.

The stakes are clear, but so are the solutions:



### **Technical action must begin now.**

Cryptocurrencies don't need to wait for perfect solutions; they can adopt post-quantum schemes in phases, ensuring flexibility for future standards. Bitcoin's Taproot upgrade has already proven that incremental improvements are possible. The next step is integrating quantum-resistant alternatives. Projects like QANplatform and IOTA have already successfully implemented post-quantum signatures, showing that the technology is ready and that what is needed is scalable deployment.



### **Collaboration across the ecosystem is essential,** but it is also a strength. No

single entity can secure Bitcoin or other cryptocurrencies alone. However, by working together, exchanges, wallet providers, miners and developers can create a model of decentralised cooperation that sets a standard for other industries. By prioritising high-risk UTXOs, testing PQC implementations and advocating for regulatory clarity, the goal is to prove that decentralised systems can evolve without sacrificing security or trust.



### **Transparency and education are key to maintaining trust.**

Developers, exchanges and wallet providers have a unique opportunity to strengthen user relationships by clearly communicating risks, timelines and safeguards. The key is preparing to ensure blockchain networks remain the most secure and innovative in the world. Clear roadmaps, accessible explanations and early miner engagement will prevent panic and ensure smooth adoption.



### **Cryptocurrencies will not collapse,** but their trustless nature demands proactive defence. The quantum threat

is not merely a distant possibility – it is a looming deadline that offers an opportunity to prepare. The time to act is now. By upgrading infrastructure, educating users and fostering collaboration, the crypto ecosystem can emerge stronger, demonstrating that decentralised networks can adapt to existential threats while preserving their core principles.

Rather than waiting for quantum computers to arrive, now is the time to build a quantum-resistant future. Cryptocurrencies and blockchain technologies will not disappear because of quantum computing; they will evolve to adapt to the coming risks. Acting today protects against future threats and lays the foundation for a safer, more resilient and more trustworthy crypto ecosystem.

## VI. Policy guidelines

01. Ensure policymakers have **access to clear, up-to-date information** on the current state and limitations of quantum computing, to allow them to better estimate/assess when a large-scale quantum computer will be achieved and when it will be able to break current cryptographic systems.

---

02. **Prioritise discussions on migrating to post-quantum cryptography** (PQC) and other quantum-resistant protocols. Engage a wide range of relevant stakeholders to determine the optimal timing for this migration.

---

03. **Establish a collaborative working group** led by the European Commission to address quantum computing challenges. Include experts from academia, the private sector, member states and relevant EU agencies (e.g. Europol, ENISA, CERT-EU, EU-AMLA). The group should produce informative assessments tailored to high-level policymakers on a regular basis, to facilitate a coordinated EU response.

---

04. Policymakers and SMEs should **closely monitor the development of central bank digital currencies** (CBDCs) and their potential impact on blockchain security, and assess their vulnerability to quantum computing threats. In Europe, close cooperation between relevant public and private stakeholders and the European Central Bank (ECB) is crucial for ensuring effective regulatory frameworks and robust security against quantum computing threats.

---

---

**QUANTUM COMPUTING AND CRYPTOCURRENCIES – BRIDGING TECHNICAL  
EXPERTISE AND DECISION-MAKING**

PDF | ISBN: 978-92-9414-127-9 | DOI: 10.2813/9406240 | QL-01-26-017-EN-N

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2026

© **European Union Agency for Law Enforcement Cooperation, 2026**

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

**Cite this publication:** Europol, Quantum Computing and Cryptocurrencies – Bridging technical expertise and decision making, Publications Office of the European Union, Luxembourg, 2026.

**This publication and more information on Europol are available on the Internet.**

[www.europol.europa.eu](http://www.europol.europa.eu)