NORTON ROSE FULBRIGHT

# Blockchain Law

# Will there be any "quantum of solace" when quantum computing comes to crypto?

New York Law Journal

July 28, 2026 | By **Robert A. Schwinger**

**James Bond creator Ian Fleming coined the phrase "quantum of solace" in his 1960 short story collection *For Your Eyes Only* as meaning "the minimum amount of comfort or peace required for a relationship to survive."**

With issues now being raised about whether quantum computing advancements might soon shatter the very technological foundation upon which cryptocurrency and other blockchain systems rely, we must ask: Can crypto still sustain a "quantum of solace" when quantum computing comes to crypto?

## Background: "Q Day"

The security of cryptocurrency networks is built on advanced encryption systems designed to protect the integrity of the networks and defend the transactions that take place there. These encryption systems are based on a mechanism called elliptic curve cryptography, which safeguards crypto transactions using a public key-private key pairing as the access code.

The pairings operate with a public key that is published the first time a crypto owner executes a trade, and a private key that remains exclusively with the owner and is used to confirm ownership of the crypto asset. The public key therefore becomes exposed as soon as an owner transacts with a crypto asset, but the private key stays hidden to ensure the asset's security.

The public key-private key pairing is most vulnerable to attack during the window of time when a transaction is being executed. If an attacker can crack the private key while the public key is exposed, the attacker can hijack the transaction and broadcast a fraudulent one instead. The attack window opens and closes depending on the time it takes to verify the public key-private key pairing. With current technology, the window is open for around 9 minutes.

**Robert A. Schiwinger** is a partner in the commercial litigation group at Norton Rose Fulbright US. **Max Nettler**, an associate in the firm's litigation group, assisted in the preparation of this column.

Attorney advertising

Reprinted with permission from the July 28, 2026 edition of the *New York Law Journal* © 2026 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. www.almreprints.com – 877-257-3382 – reprints@alm.com.

During that window, both the public and private keys are exposed while the network verifies that the private key corresponds to the public key and thereby confirms that the trader is the owner of the crypto asset. The encryption mechanism remains secure during that window because of the vast number of possible public key-private key combinations.

The number is so large that, under present technology, even using all of the computers currently on earth working together, the time needed to crack the encryption would exceed the age of the universe.

So far, so good, as long as computing capabilities remain at their current state. But what happens if the computers get better, faster, smarter?

Quantum computing is advancing in that direction. Classical computing systems interpret data and solve problems using "bits," binary digits of 0's and 1's. Quantum computers, by contrast, function using "qubits." Instead of existing in either one state or the other, i.e., as 0 or 1, qubits can occupy both states simultaneously by leveraging the probability that the underlying bit is a 1 or a 0.

Quantum computers use these probabilities to eliminate wrong answers and reach correct answers far more quickly than classical computers can. See generally Dea Bankova & Julia Wolfe, "Quantum computing decrypted", *Reuters*, Dec. 14, 2023.

Concern is now mounting that quantum computers may one day—and perhaps not too far off in the future—be capable of beating the 9-minute clock. The moment in time when quantum computers become powerful enough to crack public-key encryption systems in under nine minutes, and thereby break the cryptographic foundation upon which cryptocurrency rests, is referred to as "Q Day."

## Fears that "Q Day" is soon coming

Concern over this issue ratcheted up recently when, on March 31, 2026, Google published a research study, "Safeguarding cryptocurrency by disclosing quantum vulnerabilities responsibly", that raised alarms that the "Q Day" clock may be advancing toward midnight more rapidly than expected.

The Google study concluded that "future quantum computers may break the elliptic curve cryptography that protects cryptocurrency and other systems with fewer qubits and gates than previously realized."

According to the Google study, quantum computing will be capable of beating the current cryptography within the timespan of just "a few minutes." At these speeds, quantum computers would be able to execute a 9-minute attack and crack the current cryptography. See also Javier Bastardo, "Google Finds Quantum Computers Could Break Bitcoin Sooner Than Expected", *Forbes*, Mar. 31, 2026.

## How soon might "Q Day" be coming?

Prior to the Google report, there was debate over whether developing a quantum computer sufficiently powerful to crack current cryptography was even possible in the first instance. But the new data discussed in the Google report have shifted the discussion. Instead of arguing over an "if" or a "when," the question is now the amount of time remaining before "Q Day" arrives.

Essentially concurrently with the Google report, Google security experts introduced a "2029 timeline" for migration to quantum-resistant encryption mechanisms. Heather Adkins & Sophie Schmieg, "Quantum frontiers may be closer than they appear" (Mar. 25, 2026). Google's experts explained that "[t]his new timeline reflects migration needs for the PQC [post-quantum computing] era in light of progress on quantum computing."

The U.S. National Institute of Standards and Technology (NIST), which develops cryptographic standards that govern U.S. regulators and which are widely adopted within the crypto marketplace, has adopted a similar timeline. See D. Moody, R. Perlner, A. Regenscheid, A. Robinson & D. Cooper, "Transition to Post-Quantum Cryptography Standards", NIST Internal Report NIST IR 8547 ipd (Nov. 2024). NIST recommends that the crypto industry begin to transition away from current public-key systems and toward post-quantum methods of encryption.

Similar to Google, NIST expects to initiate this transition in phases starting around 2030, as it begins requiring post-quantum algorithms. NIST sets 2035 as the benchmark to complete the transition to a post-quantum world and the disallowance of cryptography that relies on public key-private key pairings.

The White House is reacting too. In June 2026, President Trump issued two executive orders both aimed at preparing for and responding to the challenges posed by quantum computing. The first, E.O. 14412, "Securing the Nation Against Advanced Cryptographic Attacks" (June 22, 2026), emphasizes that "[t]he advent of large-scale quantum computers, particularly in the hands of adversaries, will pose a significant threat to widely used cryptographic security systems," and directs that certain transitions to post-quantum computing be put in place as early as Dec. 31, 2030.

The second, E.O. 14413, "Ushering in the Next Frontier of Quantum Innovation" (June 22, 2026), frames recent advances as a "quantum revolution" and highlights that, alongside the threat, there is also an opportunity "to solidify the Nation's position as the world's QIST [quantum information science and technology] superpower and deliver the commercial and research benefits of quantum innovation to the American people." It outlines various steps intended to move toward that goal.

## Can crypto beat the "Q Day" clock?

Competing views exist within the crypto community on the likely impact of quantum computing.

Some believe that cryptocurrencies will not suddenly fail with the advent of a quantum computer sufficiently powerful to execute a 9-minute attack. They argue that crypto networks can and will begin to gradually adopt new, post-quantum encryption mechanisms in the time between now and "Q Day." *See* David Zaslowsky, "Quantum Computing and Bitcoin: Why 'Q-Day' Is Not an Existential Threat", N.Y.L.J., Apr. 22, 2026. "The challenge," according to this view, "is not instantaneous network failure, but the complexity of transitioning existing value to new cryptographic schemes."

Even if instantaneous failure is unlikely, fears have been expressed that quantum computing could erode consumer confidence in blockchain. Quantum attacks may not be capable of breaking into all crypto wallets at the same time, but there still may be a risk that such attacks could crack enough of them to cause a panic.

Some worry that a crypto panic could result in severe damage to cryptocurrency's market value—and possibly even jeopardize blockchain's future. *See* Mitch Jackson, "Bitcoin's Security Has an Expiration Date, Its Energy Problem Has No Fix, and Many of Its Biggest Supporters Are in Prison or Pardoned", AI, Legal/Biz Tech Update!, Apr. 8, 2026. For example, Cristiano Ventricelli, vice president and senior analyst of digital assets at Moody's Ratings, expressed concern that the public response in the wake of a large-scale attack could erode cryptocurrency's market value. See Hannah Lang, "Crypto firms prepare defenses as quantum threat to encryption draws nearer", *Reuters*, July 8, 2026.

However, the world is not being caught totally off guard. Post-quantum cryptography—specifically designed for the quantum world using algorithms built to resist even those attacks launched by large-scale quantum computers — is being developed and is already being deployed in certain contexts. *See* D. Zaslowsky, supra. Indeed, NIST released a report setting standards for post-quantum cryptography in 2024, nearly 18 months before the Google report raised concerns about the 9-minute window earlier this year.

Indeed, some blockchains have already started to make the post-quantum transition. One, the "Quantum Resistant Ledger," as its name suggests, was developed from the outset using post-quantum algorithms. A number of coins from the pre-quantum era have begun testing initial deployments of quantum-resistant technology. See *Harry Donnelly*, "Risk Frontiers: What Google's Quantum Paper Actually Means for Crypto" (Apr. 3, 2026). These early moves "are proof points that migration is technically possible."

But not all coins have moved as swiftly. Reuters reports that "[n]one of the top 20 blockchains have implemented a post-quantum signature algorithm." See *H. Lang, supra*. But some of the slower-moving coins are beginning to adapt.

For example, while Bitcoin has not adopted to date either of the standards set by NIST, see *M. Jackson*, supra, in February 2026 it has implemented "Bitcoin Improvement Proposal 360" (BIP-360), a proposal for quantum-resistant cryptography that represents its first step toward transitioning to post-quantum addresses. See J. Bastardo, supra.

But there are many cryptocurrencies and many blockchains. Whether eventual action will come too late for some or most of them is unclear.

## Is it clear that post-quantum computing or other tactics will solve the problem?

Despite these efforts, there is concern in some quarters about the viability of post-quantum technology. According to one Substack commentator, post-quantum cryptography in its present form results in "fewer transactions per block, slower throughput, and significantly higher costs across the entire network." See *H. Donnelly, supra*.

Moreover, "deployment in blockchain systems is still early," meaning "[p]erformance, software implementation, and edge cases are still being worked through in real time." Indeed, "[m]any crypto executives also warned that moving too early could create vulnerabilities because post-quantum cryptography is still rapidly evolving." See *H. Lang, supra*.

Nevertheless, crypto developers have been racing to outmaneuver the quantum threat and beat the "Q Day" clock. According to one report, a recently-unveiled crypto product is designed to "tackle quantum computing risks using a smart contract layer that runs alongside Bitcoin without requiring any change to the network itself." Shaurya Malwa & Jamie Crawley, "New wallet offers way to tackle Bitcoin's quantum risk without a fork", *CoinDesk*, Apr. 28, 2026. Proponents see this type of technology as especially promising for coins like Bitcoin that have not been at the forefront of the move toward post-quantum cryptography.

Even those who are optimistic about post-quantum technology still recognize that challenges lie ahead. Regardless of whether post-quantum technology is viable, the transition to it will take time. The shift to a post-quantum world in any event "would be more complex than prior cryptographic upgrades," and "success would depend not only on code, but on widespread user participation and social consensus." See *D. Zaslovsky, supra*.

One view is that the likely outcome for pre-quantum blockchains will be the adoption of consensus-based changes referred to as "soft forks." A soft fork involves a cryptographic update that remains compatible with pre-existing crypto assets but simultaneously introduces new rules that are more restrictive than the old ones.

The approach allows old coins to remain valid after the update, and therefore avoids forcing a split in the blockchain. So long as consensus is reached prior to the update, the existing blockchain can remain unified. Various blockchains have successfully implemented significant changes over the years through the use of soft forks. See *D. Zaslovsky, supra*.

That being said, there have been instances where attempted soft forks have not proved successful because consensus could not be reached, resulting in blockchains being split in what is called a "hard fork," such as when Bitcoin hard-forked in 2017 and split into Bitcoin Cash in a dispute over block size.

Whether making a post-quantum transition will present an even greater challenge—or an easier one because it will seem more necessary and less discretionary—remains to be seen. If many tokenholders share the view that such a transition "would be one of the most consequential changes in Bitcoin's history," see *Donnelly, supra*, the outcome may be far from certain.

## What is the correct approach?

Like the diversity of views on the crypto community's ability to adapt ahead of "Q Day," there is also debate over the correct response to the quantum threat.

The response problem is complicated by the fact that the emerging threat does not affect all coins equally. The coins associated with public keys that have already been published to the blockchain are the most vulnerable. On the other hand, public key-private key pairings that have never been used are less susceptible to quantum attacks. See *M. Jackson, supra*. The risk profiles differ because many believe that attackers are already identifying exposed public keys and storing them

to leverage by harvesting data once "Q Day" arrives. See Joseph Raczynski, "The Quantum Cryptographic Singularity: 2026's 'Checkmate' Moment", Joe Technologist, Mar. 31, 2026.

The question therefore becomes not only whether it is possible to implement quantum-resistant security, but also how to account for the different threat levels to different coins.

One view is that the safest approach is to remove exposed coins before they are stolen in a quantum attack, essentially forcing a hard fork. One proposal based on such an approach is to "phase out quantum-vulnerable addresses on a fixed five-year timeline and freeze coins that fail to migrate." See *Malwa & Crawley, supra*.

The solution, however, is potentially complicated by what is referred to as the "lost coins" problem. The issue stems from the fact that crypto networks cannot unilaterally transition coins to new quantum-resistant addresses. Coins cannot be moved without their private key, which is held exclusively by the coin's owner.

For many cryptocurrencies, including Bitcoin, meaningful portions of the blockchains are located in addresses for which the private keys have been lost. Even a consensus-based soft fork would therefore eliminate these coins from their blockchains. See *D. Zaslovsky, supra*.

Advocates of removing all exposed coins from their blockchains—regardless of soft or hard fork, or the lost coins problem—emphasize the security threat posed by vulnerable tokens. These crypto commentators highlight what they view as the significant scale of this threat for Bitcoin in particular. The pseudonymous Bitcoin inventor Satoshi Nakamoto reportedly holds exposed coins comprising approximately 5% of the total Bitcoin supply that are valued at roughly $75 billion.

This fact that raises concerns about potential consequences if a wallet that size is stolen in a quantum attack. See Jeff John Roberts, "A quantum threat to Bitcoin has some asking the unthinkable: Is it time to freeze old wallets belonging to Satoshi Nakamoto?", *Fortune*, Apr. 6, 2026.

Others, however, believe that forcibly removing coins from the blockchain is a dangerous solution in itself. They take the view that destroying coins "sets a precedent for what the protocol can do to assets it decides are inconvenient," see H. Donnelly, supra, and that "a governance strategy that entails destroying someone else's coins is anathema to Bitcoin values of self-sovereignty and decentralization." See *J.J. Roberts, supra*.

Instead of confiscating vulnerable crypto assets, another proposed solution is to create incentives for owners to voluntarily move those assets to addresses protected by post-quantum cryptography. The key is to ensure that owners make the transition before quantum attackers seize vulnerable coins, an approach dubbed a "managed migration window."

Within this window, crypto networks can impose rate-limit spending on coins associated with exposed public keys and thereby gradually encourage owners to migrate these assets to quantum-resistant addresses. Advocates highlight that a managed migration window approach avoids confiscating coins and also minimizes supply shock to the network. See *H. Donnelly, supra*.

Binance founder Changpeng Zhao has outlined a similar approach, under which a migration window of six months to a year would be established for owners to move their coins to quantum-resistant addresses. Zhao suggests that, once the migration window has closed, the network community could vote on whether the remaining pre-quantum coins should be destroyed. See Roger Satterfield, Bitcoin Experts Split on Satoshi Freeze as Quantum Threat Crosses 34% of Supply, TechTimes, July 4, 2026.

Another similar proposal is BIP-361, an enforcement-mechanism counterpart to BIP-360 that Bitcoin published in April 2026. While not yet adopted and still designated as being in draft status, BIP-361 would prohibit sending funds to quantum-vulnerable addresses by 2029, and would completely freeze pre-quantum coins by 2031. See *R. Satterfield, supra.*

## The legal fray that might result

It's often said that one should hope for the best but plan for the worst. From a liability standpoint, what might happen if "Q Day" arrives before critical blockchain infrastructure has made the necessary transition to post-quantum computing? The permutations of potential claims that might result could well be wide-ranging.

## Claims between transaction participants

The most fundamental risk is that a bad actor may be able to alter blockchain records of past or pending transactions, or place entirely fictitious transactions on the chain. Such scenarios could give rise to claims between the transaction parties, or the putative parties to a transaction that is not in fact real.

There could be any number of potential claims that might be raised between those persons, that may be based on either the reality of what happened, or on those persons' good-faith attempts to surmise (perhaps correctly, perhaps not) what had given rise to the altered or fictitious transaction records.

Claims that might be asserted in this context may include breach of contract, conversion, money had and received, and unjust enrichment. If the altered records involved "controllable electronic records" subject to UCC Article 12, claims might be asserted with respect to those digital assets under various provisions of UCC Articles 3, 4 and 4A that govern negotiable instruments, bank payments and funds transfers.

There may also be various claims in tort. Possible allegations arising from the effects of a quantum attack could include fraud, fraudulent misrepresentation, negligence (e.g., in the handling of private key data or in establishing system security protocols), and tortious interference with contractual relations.

Statutory claims might be raised under various state statutes governing deceptive or unfair trade practices. In addition, claims might be asserted under the private right of action provided by the Computer Fraud and Abuse Act, 18 U.S.C. §1030(g), for injuries caused by unauthorized access to computer systems.

If the activity giving rise to the loss is not just a one-time event but part of a regular ongoing activity, private civil RICO claims under 18 U.S.C. §1962(c) raising allegations of engaging in a "pattern of racketeering activity" might result, based upon alleged RICO predicate acts such as wire fraud under 18 U.S.C. §1343, or even financial institutions fraud under 18 U.S.C. §1344, if any kind of financial institution (as defined in 18 U.S.C. §20) were to be affected. See generally 18 U.S.C. §1961(1).

The relief that might be sought between these various parties or putative parties could be wide-ranging. Such relief might include contract damages, tort damages, restitution, disgorgement, reformation of the putative transaction, rescission, and imposition of a constructive trust. Punitive damages might be sought, and in the event of RICO claims, an award of treble damages for the injuries sustained plus costs and reasonable attorneys' fees, per 18 U.S.C. §1964(c).

## Broader systemic claims

Liability issues from quantum attacks may not just be limited to dealings between the parties or putative parties to altered or fictitious transactions, however. For example, a party who is making use of the particular blockchain or platform who suffers injury might allege that the operators were negligent in not having secured the system sooner against such quantum attacks.

They might allege that they were induced to conduct activity based on assurances of security that proved to have been unfounded. They may allege that disclosures needed to have been made to them about the risks they would face when "Q Day" arrived.

Injured persons may also point to the language used by promoters, developers, and others if they had ever touted blockchain-based records and systems using terms such as "secure," "immutable," or the like. Persons who were injured may allege that such statements were made negligently or even recklessly, given what has been generally understood about "Q Day" risks.

If quantum attacks on a particular blockchain occur with enough frequency that reliance upon the integrity of that blockchain is no longer feasible at all, parties might allege that this state of affairs amounts to force majeure, or changed circumstances, or frustration of purpose. If both sides had never thought of such events or simply assumed they could never occur, claims grounded in principles of mutual mistake might be made.

## Is there even an asset if there is no longer a viable technology?

There is also ultimately an almost metaphysical issue that a "Q Day" event might raise, because of the very nature of digital assets themselves.

It is sometimes argued that the "Q Day" problem is no worse for blockchain-based digital assets than any other financial assets, because those assets too are commonly based in bank or brokerage accounts that rely on encryption systems that could be hacked in a quantum attack. See *H. Donnelly, supra*. But there is a fundamental difference at play in the case of digital assets.

Most other financial assets have an existence independent of whatever digital technology they may now use. Assets like bank deposits, financial instruments and shares of stock existed long before there was ever digital technology. They will not cease to exist in any legal or practical sense just because the system in which they are currently housed has been hacked.

Cryptocurrencies and other digital assets, by contrast, only exist within the blockchain technology that gave birth to them and support them. Does a coin have any existence, or value, or legal status, if there is no longer any reliable and functional blockchain underlying it?

If that happens, it may be difficult even to conceptualize what kind of injury, if any, this might be to the tokenholder, and who in the decentralized blockchain system could be said to have been under a duty to guard against it.

## Conclusion

"Q Day" is coming, and it threatens both conceptual conundrums and substantial injuries if successful quantum attacks on blockchain systems can occur before quantum-resistant systems can be introduced. With luck, the industry will move fast enough to avoid having to confront these issues — rather like James Bond defusing a bomb at the last moment. For now, however, we remain in the riveting suspense stage where the audience agonizes over whether catastrophe will be averted, so that crypto can continue to enjoy a "quantum of solace."

NORTON ROSE FULBRIGHT

Norton Rose Fulbright provides a full scope of legal services to the world's preeminent corporations and financial institutions. The global law firm has more than 3,000 lawyers advising clients across locations in the United States, Europe, Canada, Latin America, Asia, Australia, Africa and the Middle East.

**nortonrosefulbright.com**

The purpose of this communication is to provide information as to developments in the law. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.

Norton Rose Fulbright © 2026. All Rights Reserved
72548-US- 07/26