# Macro shocks, leverage and crypto's quantum uncertainty

Veröffentlicht am 9. Februar 2026

**Elvira Kuramshina**
Associate Director, Quantitative Research

**Blake Heimann**
Associate Director, Quantitative Research

## Wichtige Erkenntnisse

- Leveraged liquidations have amplified recent crypto drawdowns, a dynamic that has historically been followed by stabilisation or recovery.
- Recent underperformance reflects not only macro and leverage pressures, but rising awareness of longer-term structural risks, including quantum computing.
- Quantum risk is systemic, extending beyond crypto to traditional financial institutions and digital infrastructure.
- Ethereum has moved early on post-quantum security, positioning the network ahead of an industry-wide transition.
- The growth of the quantum computing ecosystem, including post-quantum cryptography, reflects rising efforts to mitigate quantum-driven security risks across digital infrastructure.

Recent leveraged liquidations in crypto markets highlight how macro catalysts can interact with elevated leverage to produce outsized volatility. Ethereum is currently trading near $2,100, its lowest level since mid-2025, following a sharp drawdown that coincided with President Trump’s nomination of Kevin Warsh as Federal Reserve Chair. Markets interpreted the move as reinforcing a regime of tighter monetary policy, triggering a broader risk-off rotation.

More than $2 billion in ETH positions were liquidated in a single day, with forced selling amplifying the decline. Stress also appears to have extended beyond derivatives markets, as digital asset treasury firms and crypto-native corporates holding liquid tokens face pressure to de-risk, adding to near-term selling pressure.

## Figure 1: Ether (ETH) Historical price action after major crypto liquidation events

*Source: Artemis, WisdomTree, as of February 3, 2026. Past performance not indicative of future results.*

Large liquidation events typically unfold in stages and can create oversold conditions. The table shows the ten largest episodes since 2021; in seven of the eight cases with complete six-month data, Ethereum prices were higher six months later.

Past patterns are not guarantees and the macro backdrop has evolved, but Ethereum's core drivers remain intact. Asset tokenisation continues, regulatory clarity is improving—including momentum around the CLARITY Act—and broader crypto adoption persists through expanded access.

Periods of forced deleveraging also prompt investors to reassess structural assumptions. In crypto, security is foundational: without confidence in cryptographic integrity, liquidity and adoption ultimately falter. It is in this context that an underappreciated long-term risk comes into sharper focus: quantum computing.

## Beyond volatility: Quantum resilience

Beyond these macro dynamics, an emerging structural risk has been weighing on the crypto ecosystem: the potential for quantum computing to undermine current public-key cryptography. Over recent months, some investors have increasingly framed crypto's relative underperformance through the lens of growing quantum-related concerns.

In January, Ethereum elevated post-quantum security to a strategic priority. The Ethereum Foundation established a dedicated team, accelerated R&D, and launched million-dollar incentives for quantum-resistant solutions. This positions the network ahead in preparing for the transition.

Quantum risks are not crypto-specific; they threaten encryption across traditional finance and global markets. Decentralized protocols face unique upgrade coordination challenges, making early action particularly valuable. While crypto experiences this risk in an acute, open form, the threat is systemic for legacy institutions, corporates, and infrastructure.

## Quantum risks and the push for post-quantum security

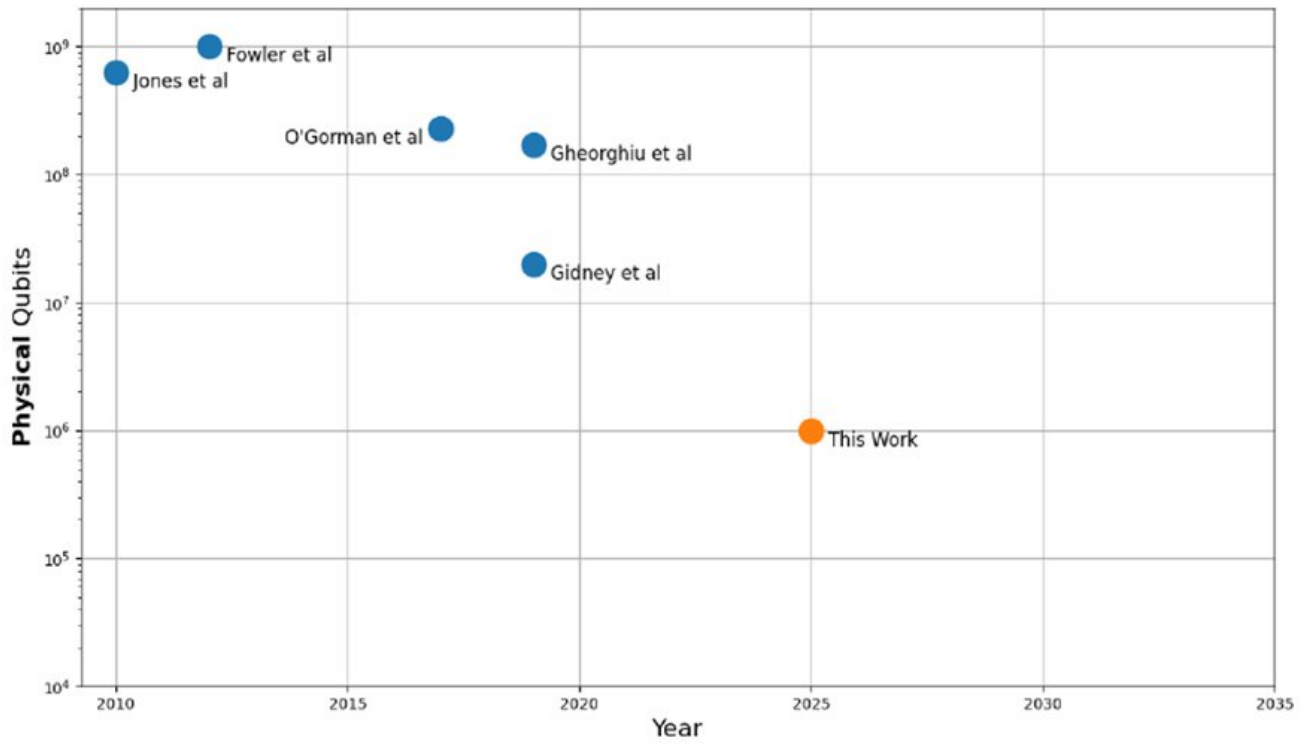
Momentum in quantum computing has accelerated meaningfully in 2025, pushing what was once a theoretical risk firmly into the realm of strategic planning. Governments and the quantum industry are now openly aligning around timelines that point to the early 2030s for so-called "cryptographically relevant" quantum machines. As awareness grows, so does recognition of the threat quantum computing poses to modern cryptography – the security backbone not only of digital assets and blockchains, but of virtually all encrypted systems today.

At the core of the issue is Shor's algorithm, which, once run on a sufficiently powerful fault-tolerant quantum computer, could efficiently break widely used public-key cryptography such as RSA and elliptic curve cryptography (ECC). ECC, in particular, is foundational to blockchain wallets, transaction signing, and key management across the digital asset ecosystem. While today's quantum machines remain far from this capability, the direction of travel is clear and is accelerating.

That acceleration is increasingly visible in both academic research and industry roadmaps. In a 2025 paper, Google showed that the estimated number of physical qubits required to execute Shor's algorithm has

fallen by roughly 20x compared with a 2019 baseline, as illustrated in Figure 2. At the same time research and tech breakthroughs align with increasingly concrete industry timelines. Leading quantum companies such as IonQ and PsiQuantum have publicly articulated plans to deliver machines with on the order of one million physical qubits by the end of the decade. While a range of complex engineering challenges remain and timelines may shift as the technology matures, these roadmaps nonetheless place the emergence of cryptographically relevant quantum computers firmly within an investable time horizon.

## Figure 2: Historical estimates, with comparable physical assumptions, of the physical qubit cost of factoring 2048 bit RSA integers.




Source: Google Quantum AI, Craig Gidney “How to factor 2048 bit RSA integers with less than a million noisy qubits”.

Critically, the threat is not limited to the moment a quantum computer switches on. “Harvest now, decrypt later” strategies mean encrypted data and blockchain activity recorded today could be vulnerable in the future. This is why the quantum industry, in close coordination with standards bodies such as the U.S. National Institute of Standards and Technology (NIST), has already moved from theory to implementation. In August 2024, NIST formally approved the first three PQC algorithms, marking a critical milestone in the rollout of cryptographic standards designed to remain secure against both classical and quantum attacks.

## Hedging quantum risk with quantum exposure

One way to potentially hedge against quantum-driven security risks is to gain exposure to the quantum computing industry itself and the growth it is expected to unlock. Within that landscape, post-quantum cryptography plays a distinct and strategically important role. While PQC does not directly contribute to the development of quantum hardware or algorithms, it is closely tied to continued progress in quantum computing, as each breakthrough increases the urgency of securing existing digital infrastructure. This creates an opportunity to capitalise on quantum-related advances in the near term, i.e. well before the full onset of a quantum era, because cryptographic migration must begin ahead of “Q-Day,” not after it.

Even under conservative assumptions, large-scale migration to post-quantum standards is expected to take multiple years, a reality increasingly reflected in coordinated guidance across major jurisdictions, including the United States, the United Kingdom, and the European Union (see Figure 3), urging organisations, particularly those operating critical or systemically important infrastructure, to begin quantum-readiness planning and post-quantum migration now. For crypto networks in particular, where cryptographic security underpins trust, liquidity, and adoption, the transition to post-quantum standards represents not just a technical upgrade, but a critical component of long-term resilience.

## Figure 3: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography issued by the EU Member States.

*Source: European Commission press release from 23 June 2025 available at EU reinforces its cybersecurity with post-quantum cryptography | Shaping Europe’s digital future.*

## Important Risks Related to this Article

# Important Information

**Marketing communications issued in the European Economic Area ("EEA"):** This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

**Marketing communications issued in jurisdictions outside of the EEA:** This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

**For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.**

The application of regulations and tax laws can offen lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.