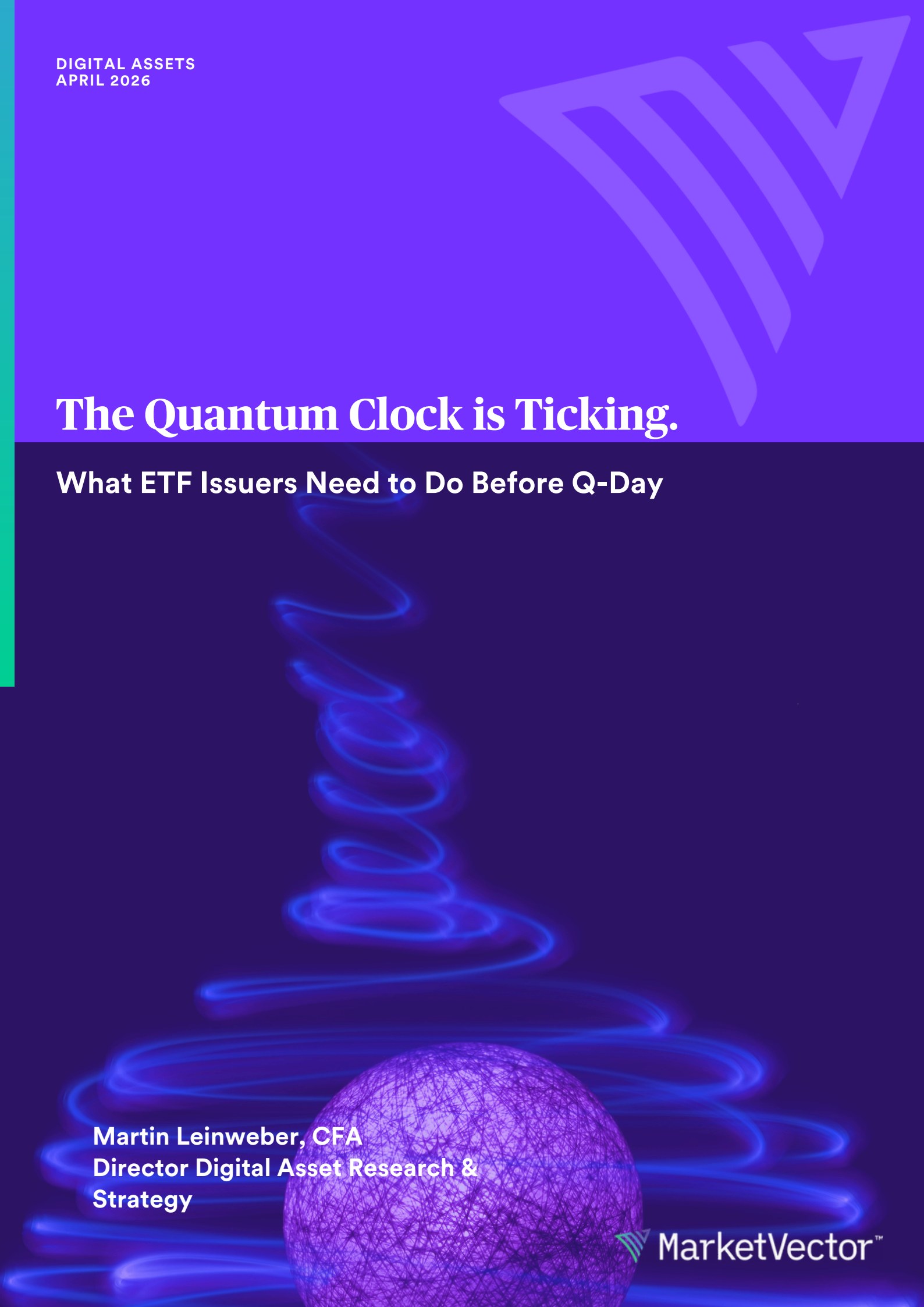
DIGITAL ASSETS
APRIL 2026

The Quantum Clock is Ticking.

What ETF Issuers Need to Do Before Q-Day



Martin Leinweber, CFA
Director Digital Asset Research & Strategy

MarketVector™

Contents

The Quantum Clock Is Ticking.

Bitcoin Cracked in 9 Minutes: What ETF Issuers Need to Do Before Q-Day

EXECUTIVE SUMMARY

> *Google just moved the quantum timeline forward. The real risk for ETF issuers isn't the cryptography. It's the fork.*

Google's March 2026 research materially lowered the estimated hardware threshold for breaking current cryptography, while roughly 6.9 million BTC is already held in addresses potentially vulnerable to a quantum attack.

For ETF issuers, the risk extends well beyond the Bitcoin protocol itself. Custodians, index methodologies, and NAV processes all rely on cryptographic assumptions that could be disrupted — yet no major custodian has publicly completed a post-quantum migration plan. A quantum-triggered Bitcoin upgrade would likely require a contentious fork, creating significant legal, operational, and valuation challenges for issuers.

Ethereum may be better positioned because its account abstraction framework allows wallet-level migration to post-quantum security, whereas Bitcoin would likely need a slower, governance-heavy network-wide transition. Research suggests Bitcoin's migration could take 10–15 years — which may be longer than the available window.

MarketVector is treating quantum preparedness as a core responsibility. The firm is reviewing index fork provisions, building an internal fork-monitoring framework, tracking BIP-360, and assessing whether the Bitcoin Benchmark Rate should include additional quantum-specific language.

For ETF issuers, the immediate priority is preparedness: obtain formal custodian migration plans, confirm index methodologies can handle compromised supply and forks, test chain-split scenarios operationally, monitor emerging Bitcoin proposals, and prepare clear investor communications in advance.

1. The Threat, Explained Simply

The cryptographic architecture securing virtually all digital assets today rests on a single mathematical assumption: that deriving a private key from a public key is computationally infeasible. Bitcoin, Ethereum, and the vast majority of blockchain networks rely on elliptic curve cryptography (a family of public-key algorithms based on the algebraic structure of elliptic curves over finite fields) to generate digital signatures. The specific curve Bitcoin uses, known as secp256k1, produces key pairs in which the private key can generate the public key through a one-way mathematical function. Reversing that operation, with today's classical computers, would take longer than the age of the universe.

Quantum computing changes this calculus. In 1994, mathematician Peter Shor published an algorithm that, if executed on a sufficiently powerful quantum computer, can solve the discrete logarithm problem (the mathematical foundation underpinning elliptic curve security) exponentially faster than any known classical method.[i] A useful analogy: classical computers attempting to reverse a public key are trying every possible combination on an enormous lock, one at a time. A quantum computer running Shor's algorithm can, in effect, test many combinations simultaneously through the quantum mechanical property of superposition, reducing what would be a trillion-year task to a matter of minutes.

For digital asset markets, the threat manifests in two distinct attack vectors. The first is the so-called harvest-now-decrypt-later scenario, where adversaries collect encrypted data today with the intent of decrypting it once quantum hardware matures. While relevant for communications security, this is less directly applicable to blockchain transactions. The second vector, and the critical one for asset owners, is the active key attack: deriving a private key from an exposed public key in real time, then signing fraudulent transactions before the legitimate owner can respond. In Bitcoin, a public key is exposed the moment a wallet initiates a transaction and broadcasts it to the network mempool. For legacy pay-to-public-key (P2PK) addresses, which include an estimated 1.72 million coins from Bitcoin's earliest years and potentially Satoshi Nakamoto's holdings of roughly one million BTC, the public key has been permanently visible on-chain since the day those coins were mined.

> *"The window for preparation is narrowing, and the rate of improvement in quantum hardware, error correction, and algorithmic optimization has consistently outpaced prior forecasts.*

Until recently, expert consensus placed the arrival of a cryptographically relevant quantum computer (a machine powerful enough to run Shor's algorithm at scale against 256-bit elliptic curves) somewhere between 2040 and 2060. That timeline has compressed substantially. In March 2026, Google's Quantum AI team published research demonstrating that breaking the elliptic curve cryptography used by Bitcoin wallets could require fewer than 500,000 physical qubits, roughly a twentyfold reduction from prior estimates that assumed millions of qubits would be necessary.[ii] This does not mean the threat is imminent. Current quantum processors operate with approximately 1,000 to 1,500 noisy, non-fault-tolerant qubits, well below the threshold required for a practical attack. However, the honest assessment is this: the window for preparation is narrowing, and the rate of improvement in quantum hardware, error correction, and algorithmic optimization has consistently outpaced prior forecasts.

2. Why This Is an ETF Operations Problem, Not Just a Tech Problem

For institutional investors, the natural impulse is to classify quantum risk as a purely technical issue, something for protocol developers and cryptographers to resolve. That framing is incomplete. A quantum-capable adversary does not distinguish between bitcoin held in a self-custody wallet, a spot ETF's custody arrangement, or a fund administrator's settlement pipeline. The risk permeates every layer of the value chain.

Custody risk is the most immediate operational concern. Prime custodians serving spot bitcoin ETFs, including Coinbase Custody, BitGo, and Fidelity Digital Assets, hold client assets in wallets secured by the same elliptic curve cryptography that a quantum computer would target. If a custodian's wallet infrastructure has ever reused addresses or exposed public keys through operational processes, those specific holdings become vulnerable. Migration to quantum-resistant wallet formats requires not only new cryptographic libraries but also updated hardware security modules, revised key management procedures, and potentially new insurance frameworks. No major custodian has publicly disclosed a completed post-quantum migration plan as of early 2026. The question ETF issuers should be asking their custodians today is straightforward: what is your post-quantum migration roadmap, and what is your contingency plan if a quantum-capable computer appears earlier than your timeline assumes?

Index integrity presents a more subtle but equally important challenge. Index providers track digital assets by their on-chain footprint, and methodologies for calculating free-float supply, circulating supply, and market capitalization depend on assumptions about which coins are accessible and which are effectively lost. If quantum attackers compromise large dormant

wallets, including Satoshi's estimated one million BTC, the market faces an ambiguous scenario. Do those coins count as "recovered supply" that increases the denominator for market cap calculations? Or are they stolen property that should be excluded? Most index methodologies in the digital asset space do not have explicit provisions for cryptographically compromised supply. At MarketVector, this is a gap we have identified and are actively working to address across our index suite. Our view is that index providers have a responsibility to think through these scenarios before they arrive, not after.

> *"The window for preparation is narrowing, and the rate of improvement in quantum hardware, error correction, and algorithmic optimization has consistently outpaced prior forecasts.*

NAV uncertainty compounds the problem. A large-scale quantum theft event, or even a credible public demonstration of the capability, would likely trigger severe price dislocation. The creation and redemption mechanisms that keep ETF prices aligned with net asset value depend on functioning markets with reasonable bid-ask spreads. During a quantum panic, authorized participants might withdraw from market-making activity, causing the premium or discount to NAV to blow out in ways that ETF issuers have not stress-tested. This is not a hypothetical: the March 2020 COVID-driven dislocation in fixed-income ETFs demonstrated how quickly the creation-redemption arbitrage mechanism can break under extreme stress. For a historical parallel in crypto, Exhibit 4 below shows how Bitcoin's market cap dominance collapsed from 96% to 37% during the 2017 fork war, illustrating how fork-driven uncertainty does not stay contained within the forking asset but bleeds into the entire digital asset market.

3. The Fork Scenario: The Block Size War as Reference Point

The most likely path to quantum resistance for Bitcoin involves a protocol upgrade that introduces post-quantum signature schemes. This could take the form of a soft fork (a backward-compatible change that tightens the existing rules, allowing upgraded and non-upgraded nodes to coexist) or a hard fork (a backward-incompatible change requiring all participants to upgrade). BIP-360, the most mature proposal currently under development, envisions a soft fork that introduces a new output type called Pay-to-Quantum-Resistant Hash, designed to allow voluntary migration to quantum-safe addresses. Unlike Ethereum, which has account abstraction (a protocol-level mechanism allowing wallets to adopt arbitrary signature schemes without requiring a network-

wide fork) as a more flexible upgrade path, Bitcoin's conservative governance culture makes any protocol change politically contentious. This conservatism has historically been a strength, ensuring stability and resistance to capture. In a quantum threat scenario, it may become a liability.

The most instructive precedent is the 2017 block size war, a governance crisis that ultimately produced a hard fork. The disagreement centered on whether to increase Bitcoin's block size limit to accommodate more transactions per block, a seemingly straightforward technical question that devolved into a bitter ideological conflict about Bitcoin's purpose and governance. The dispute culminated on August 1, 2017, when a faction of the community activated Bitcoin Cash (BCH) as a separate chain. As Exhibit 1 illustrates, the months that followed were marked by genuine uncertainty. The BCH/BTC price ratio (Exhibit 2, lower panel) initially spiked to 14% at the fork, then collapsed to 5% by mid-October, before surging to 26% during the November "flippening" scare when SegWit2x was cancelled and hash rate temporarily migrated from BTC to BCH. The BTC hash rate itself showed a visible dip around August 28, when miners temporarily shifted computing power to the more profitable BCH chain.

Exhibit 1: *The resolution window — BTC and BCH price action with key events annotated (Jul 2017 – Jun 2018). The shaded regions indicate the uncertainty phase (fork to SegWit2x cancellation) and resolution phase (SegWit2x cancellation through market-wide correction).*

The signals that ultimately resolved the question of which chain was "Bitcoin" included hash rate distribution (how much mining power secured each chain), exchange listings and price discovery, developer activity and alignment, and the behavior of major economic actors like custodians and payment processors. Bitcoin (BTC) retained dominance, and BCH became a secondary asset. But as the data show, the process of establishing that outcome took roughly three to six months of sustained market uncertainty, during which ETF issuers and index providers would have faced acute operational challenges.

Exhibit 2: *BTC and BCH price discovery (top) and BCH/BTC dominance ratio (bottom). The ratio peaked at 26% during the November 2017 flippening scare before declining steadily through Q1 2018, ultimately settling below 10%.*

A post-quantum fork scenario could prove considerably more complex. Where the block size debate was relatively binary (bigger blocks versus the status quo), the quantum threat introduces multiple competing proposals with different technical approaches, risk tolerances, and timelines. BIP-360 proposes a cautious, soft-fork path focused on new address types. The "Hourglass" proposal suggests rate-limiting spends from vulnerable addresses to slow the impact of a quantum attack without outright freezing coins. Jameson Lopp's more aggressive proposal would phase out quantum-vulnerable address formats entirely, eventually rendering unmigrated coins unspendable. And a faction of the community may argue that no action is necessary at all, that

the threat is overstated or that Bitcoin's market dynamics will self-correct. In this environment, a single clean fork is not guaranteed. Multiple competing chains could emerge simultaneously: a "conservative" fork that delays migration, an "aggressive" fork that moves fast, and the incumbent chain that makes no changes.

How Long Does It Take to Identify the Dominant Fork?

In 2017, it took roughly three to six months before Bitcoin Cash was clearly subordinate to Bitcoin in terms of hash rate, developer activity, and market capitalization. As Exhibit 2 shows, the BCH/BTC ratio did not settle below 10% until March 2018, seven months after the fork. A post-quantum fork might resolve faster if the threat is acute and imminent, because the economic incentive to converge on the secured chain would be overwhelming. If a quantum computer is publicly demonstrated to have broken a secp256k1 key, the chain that has already deployed quantum-resistant signatures would attract hash rate and capital almost immediately. Conversely, if the threat remains probabilistic and disputed, where researchers disagree on timelines and no public demonstration has occurred, the coordination problem becomes worse than 2017. The stakes are existential rather than ideological, but the absence of a concrete trigger event makes consensus harder to achieve. The honest answer is that there is no reliable playbook for this scenario.

Signals Index Providers and ETF Issuers Should Monitor

We propose a framework organized around five categories of observable signals, each of which played a decisive role in the 2017 fork resolution.

First, hash rate migration. Which chain miners choose to secure is the most immediate indicator of where the market expects value to accrue, as miners follow economic incentives and their aggregate behavior reveals market expectations about which fork will survive. During the 2017 fork, BTC hash rate temporarily dipped as miners shifted to BCH around late August, before recovering as difficulty adjusted. In a quantum scenario, hash rate migration would signal which chain miners believe is cryptographically secure.

Second, exchange listings and withdrawal support. Exchanges must decide which fork to list under the "BTC" ticker and which to treat as a derivative asset; their decisions shape liquidity and price discovery. The 2017 fork provides a particularly instructive case study. As Exhibit 3 details, Bitfinex and Kraken listed BCH immediately on August 1, while Coinbase credited BCH balances but blocked trading for over four months, finally enabling BCH trading on December 19. That

listing triggered a spike to $3,700 and subsequent insider trading allegations. The lesson for a quantum fork: exchange support decisions are neither instant nor uniform, and the timing of those decisions can create significant price dislocations.

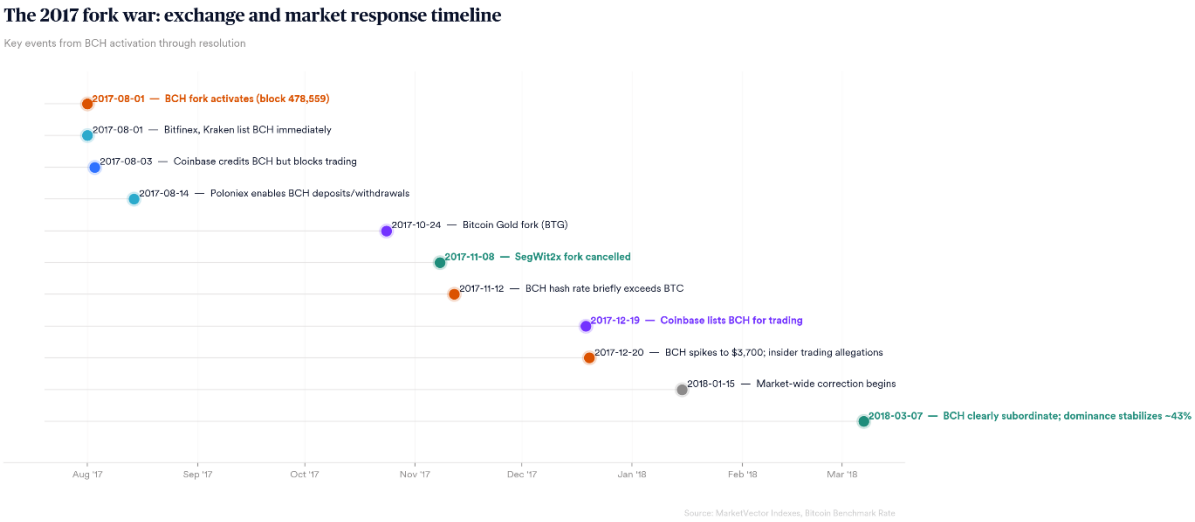


Exhibit 3: *Exchange and market response timeline during the 2017 BCH fork. Key observation: Coinbase's 4.5-month delay in listing BCH created a liquidity vacuum that, when resolved, produced extreme price volatility and insider trading concerns.*

Third, developer activity: the volume and quality of GitHub commits, BIP adoption status, and the alignment of prominent Bitcoin Core contributors signal which fork has the deepest technical credibility. **Fourth, custodian support:** institutional custodians will need to decide which fork they are willing to hold, clear, and settle for ETF clients; their decisions may lag the market but carry enormous weight. **Fifth, regulatory signals:** whether the SEC or European regulators treat a post-quantum Bitcoin fork as the same underlying asset for purposes of existing ETF and ETP approvals, or whether new filings are required, is a question with no current precedent but significant commercial consequences.

The Parallel to 2017 for Index Handling

During the 2017 fork, some index providers eventually adopted a "dominant chain" rule with a waiting period, before reclassifying the fork. ETF issuers distributed forked coins as in-kind dividends or liquidated them on behalf of shareholders. A post-quantum fork would likely require similar policies, but the urgency may compress the timeline. If the quantum threat is credible and imminent, a ninety-day waiting period may be untenable from a risk management perspective.

Exhibit 4: *Bitcoin market cap dominance (Jan 2017 – Jun 2018). Dominance declined from 96% to a trough of approximately 37% as the fork, the ICO boom, and market fragmentation compounded. A quantum-driven fork could trigger a similar or more severe dominance compression.*

The MarketVector Bitcoin Benchmark Rate (BBR), which serves as the reference rate for a number of institutional products, already incorporates fork-handling provisions. Under the current methodology, a forked coin is not added to the index; only in the event that a spun-off chain exceeds Bitcoin by market capitalization and gains general acceptance as the successor of the original chain would MarketVector consider different treatment. This framework, established in 2022 after the lessons of the BCH fork, provides a reasonable baseline. However, the quantum scenario introduces complexities that the current rules were not designed to address: multi-fork fragmentation, the possibility of exchange-level liquidity crises during the observation period, and the ambiguity of what constitutes “general acceptance” when the community is split not over ideology but over risk tolerance. We are currently reviewing the BBR methodology to determine whether supplemental provisions, specifically an explicit observation framework with defined criteria and escalation triggers for quantum-related fork events, should be added. We expect to communicate the outcome of this review to our clients and licensees in the coming months.

The critical takeaway for ETF issuers is that fork-handling policies must be developed, documented, and stress-tested before the fork occurs, not after. The 2017 experience demonstrated that ad hoc responses create legal ambiguity, operational confusion, and reputational risk. Index providers that have done this work in advance will be materially better positioned to support their clients through a quantum-driven fork event.

4. Post-Quantum Migration Proposals: What Is Being Done

Bitcoin: BIP-360 and Competing Approaches

BIP-360, authored by Hunter Beast and now merged into the official Bitcoin Improvement Proposals repository, represents the most mature Bitcoin-native approach to post-quantum security.[iii] The proposal introduces a new output type, originally designated Pay-to-Quantum-Resistant-Hash (P2QRH) and subsequently refined into a Taproot-like script tree structure with the vulnerable key-path spend removed. All spends under this new format must reveal a script path and a Merkle proof rather than a raw public key, directly targeting the long-exposure vulnerability that Shor's algorithm would exploit.

The proposal supports multiple NIST-standardized post-quantum signature algorithms. FALCON, a lattice-based scheme prioritized for its signature aggregation potential, produces signatures of approximately 1,280 bytes, roughly twenty times larger than a 64-byte Schnorr signature used in current Taproot transactions. CRYSTALS-Dilithium (now standardized as ML-DSA), another lattice-based scheme, generates signatures ranging from 2,420 bytes at NIST Level I security to 4,595 bytes at Level V. SPHINCS+ (SLH-DSA), a hash-based scheme with more conservative security assumptions, produces signatures that can exceed 29,000 bytes depending on parameter choices.[iv] For context, a typical Bitcoin transaction today is roughly 250 bytes. The practical consequence is stark: post-quantum signatures will occupy dramatically more block space, reducing transaction throughput and increasing fees, potentially by an order of magnitude.

Beyond BIP-360, several complementary proposals are under active discussion. The "Hourglass" proposal, developed by Hunter Beast and Michael Casey of Marathon, would impose a rate limit on spends from P2PK addresses, capping the amount that can be moved per block to roughly one bitcoin.[v] Under Hourglass V2 parameters, it would take more than thirty-two years to move all P2PK coins, dramatically limiting the market impact of a quantum-enabled liquidation event while preserving the theoretical spendability of those coins. Jameson Lopp's "Post-Quantum Migration and Legacy Signature Sunset" proposal takes a more aggressive approach: a phased soft fork that would first block new deposits to vulnerable address formats, then invalidate spending from those formats entirely, with an optional recovery mechanism using zero-knowledge proofs tied to seed phrases.[vi] A commit-and-reveal scheme, sometimes described as a "proof-of-quantum-computer" triggered emergency brake, represents yet another approach: it would require no changes to Bitcoin until a quantum attack is actually demonstrated, at which point pre-committed hash proofs would be required for any spend.

For index providers and ETF issuers, the practical implication of these competing proposals is significant. Each one would handle the roughly 6.9 million BTC in quantum-vulnerable addresses differently: BIP-360 enables voluntary migration, Hourglass rate-limits the damage, Lopp's proposal forces migration on a deadline, and the commit-reveal approach waits for an actual attack. The policy chosen by whichever fork prevails will directly affect circulating supply dynamics, market microstructure, and the operational assumptions embedded in index methodologies. This is not merely a developer debate. It is a question about the economic structure of Bitcoin itself.

Ethereum: Account Abstraction as Structural Advantage

Ethereum's approach to post-quantum readiness benefits from a structural advantage that Bitcoin lacks. With the activation of EIP-7702 in the Pectra upgrade of May 2025, Ethereum enabled externally owned accounts to delegate execution logic to smart contracts, effectively decoupling wallet behavior from a fixed signature scheme.[vii] The Ethereum Foundation's 2026 protocol roadmap explicitly positions native account abstraction, through proposals like EIP-8141 (Frame Transactions), as the migration path away from ECDSA-based authentication. Because account abstraction allows individual wallets to adopt post-quantum signatures without requiring a network-wide consensus change, Ethereum can migrate incrementally. Wallets upgrade on their own timeline. The network accommodates both legacy and post-quantum authentication simultaneously.

The Ethereum Foundation launched a dedicated post-quantum research portal with eight years of accumulated research, more than ten client teams shipping weekly development networks, and a multi-fork migration roadmap with specific timelines. The contrast with Bitcoin's governance posture is striking and has drawn commentary from prominent voices across the industry. The difference is not primarily technical. It is structural and organizational. Ethereum has a foundation that can fund and coordinate multi-year engineering efforts. Bitcoin's decentralized governance model, which is a feature for censorship resistance, creates a liability when facing a deadline.

> *"The difference is not primarily technical. It is structural and organizational. Ethereum has a foundation that can fund and coordinate multi-year engineering efforts. Bitcoin's decentralized governance model, which is a feature for censorship resistance, creates a liability when facing a deadline.*

The Coordination Problem

Even where technically sound solutions exist, deploying them across a decentralized network requires social consensus among miners, node operators, wallet developers, custodians, and exchanges. In Bitcoin, this consensus cannot be mandated. It must be persuaded. The history of Bitcoin protocol upgrades suggests this process takes years under favorable conditions: Segregated Witness, which offered clear performance benefits, took approximately two years from proposal to activation. Post-quantum migration is what researchers have characterized as a "defensive downgrade": it imposes immediate, measurable costs (larger signatures, higher fees, reduced throughput) in exchange for protection against a threat that remains probabilistic. Convincing a decentralized community to accept a fifty-percent capacity reduction to defend against a computer that does not yet exist is a fundamentally different governance challenge than persuading it to adopt an upgrade that makes transactions cheaper. Academic research published in 2026 estimates that realistic migration timelines for Bitcoin range from ten to fifteen years, a window that may or may not align with the arrival of cryptographically relevant quantum hardware.

5. What ETF Issuers Should Be Doing Now

The appropriate posture is not alarm. It is preparation. The institutions that develop quantum-readiness frameworks during 2025 and 2026 will be better positioned not only to manage a potential crisis but to explain it to their investors when it arrives. The following agenda items represent, in our view, the minimum standard of due diligence for any institution operating a spot digital asset ETF or ETP.

> *The appropriate posture is not alarm. It is preparation.*

Engage custodians directly. ETF issuers should request formal written responses from their custodians regarding post-quantum migration plans. Specific questions include: when does the custodian plan to upgrade wallet infrastructure to quantum-resistant formats? What signature schemes are under evaluation? What is the contingency plan if a quantum-capable computer appears earlier than the custodian's internal timeline assumes? Has the custodian conducted internal tabletop exercises modeling a quantum theft event? If the custodian cannot provide substantive answers, that itself is a finding.

Review index methodology. Does the index provider tracking the fund's underlying asset have explicit fork-handling rules? Are circulating supply calculations robust to large-scale wallet compromise events? If several million previously dormant bitcoin were to move in a short period, whether through legitimate migration or quantum theft, how would the index methodology respond? At MarketVector, our index guides already contain fork-handling provisions and explicit discretion frameworks for extraordinary events. We are enhancing these provisions with quantum-specific language, and we encourage other index providers and their licensees to undertake similar reviews.

Model the fork scenario. ETF issuers should conduct a tabletop exercise based on the following premise: Bitcoin forks in response to a credible quantum threat. One chain implements post-quantum signatures; the other does not. What is the legal obligation to investors under the fund's prospectus? What does the prospectus define as the "underlying asset"? Does it reference a specific protocol specification, or does it reference "Bitcoin" generically? How would creation and redemption units be handled during a period of chain ambiguity? The exhibits in this article, particularly the dominance compression shown in Exhibit 4 and the multi-month resolution timeline shown in Exhibit 1, should inform the assumptions used in such exercises.

Monitor the BIP process. BIP-360 and related proposals are public documents with active discussion threads. Assign someone on the product or risk team to track their status, understand the competing proposals, and report material developments. The Bitcoin development mailing list and relevant GitHub repositories are the primary sources. This monitoring function does not require deep cryptographic expertise, but it does require sustained attention.

Consider proactive disclosure. Institutional investors, allocators, and regulators may begin asking about quantum risk as part of their digital asset due diligence process. Getting ahead of this with a clear, informed, and measured position is a competitive advantage. An institution that can articulate its understanding of the quantum threat, the steps it has taken to prepare, and its framework for responding to a fork event will be more credible to investors than one that offers silence or dismissive reassurance.

6. What MarketVector Is Doing: Our Commitment to Quantum Readiness

As the provider of reference rates and index methodologies that underpin institutional digital asset products, we regard quantum preparedness as a core responsibility. We are taking the following steps.

MarketVector's quantum readiness program

1. **Index guide review.** We are conducting a comprehensive review of our index guide provisions related to forks and extraordinary events. The MarketVector Bitcoin Benchmark Rate (BBR) and our broader digital asset index suite already contain fork-handling rules and discretion frameworks developed in accordance with IOSCO Principles for Financial Benchmarks. We are evaluating whether these provisions require supplemental language to address quantum-specific scenarios, including multi-fork fragmentation, cryptographic compromise of the underlying protocol, and the potential impact of large-scale wallet vulnerability on circulating supply calculations

2. **Fork observation framework.** We are developing an internal fork observation framework with explicit criteria for identifying the dominant chain in a post-quantum fork scenario. This framework will draw on the five-signal model described in Section 3 of this article: hash rate migration, exchange support, developer alignment, custodian adoption, and regulatory treatment. Our objective is to ensure that if a quantum-driven fork occurs, our response is governed by a pre-established, transparent process rather than ad hoc judgment.

3. **Active BIP-360 monitoring.** We are monitoring the BIP-360 process and related proposals as part of our ongoing index maintenance obligations. We have assigned internal resources to track the technical and governance status of post-quantum proposals on the Bitcoin development mailing list and relevant GitHub repositories. Material developments will be assessed for their implications on our index methodologies and communicated to licensees as appropriate.

We do not believe the quantum threat requires immediate changes to our index calculations or constituent definitions. What it does require is a documented framework for responding when and if the threat materializes. We intend to be transparent with our clients about both the risks we see and the preparations we are making.

CONCLUSION

The quantum threat to digital asset cryptography is neither imminent nor imaginary. It occupies an uncomfortable middle ground: a risk that is real enough to demand preparation but uncertain enough to resist precise calibration. For ETF issuers and their index providers, the relevant question is not whether quantum computers will eventually break elliptic curve cryptography. The emerging expert consensus is that they will. The question is whether the institutions responsible for managing investor capital in digital assets have done the work to understand what happens next: to their custody arrangements, to their index methodologies, to their legal obligations, and to their ability to navigate a protocol fork that could redefine which chain constitutes "Bitcoin."

The 2017 block size war, as documented in the exhibits throughout this article, demonstrated that even ideological disputes can produce genuine economic uncertainty lasting months and compressing Bitcoin's market dominance from 96% to 37%. A quantum-driven fork, with existential rather than ideological stakes, could produce something considerably more disruptive. The institutions that have developed frameworks for responding to this scenario, that have engaged their custodians, stress-tested their index methodologies, and prepared their investor communications, will be better positioned not just to survive such an event, but to maintain the trust of the investors who depend on them.

At MarketVector, we believe that preparation is the competitive advantage. We are building the frameworks now so that our clients do not have to improvise later. We encourage every participant in the digital asset value chain, from protocol developers to custodians to asset managers, to begin the same work. The quantum clock is ticking. The time to prepare is while it is still possible to do so thoughtfully.

Contact

info@marketvector.com

About the Author

Martin Leinweber, CFA;
Head of Digital Asset Research & Strategy, MarketVector Indexes
mleinweber@marketvector.com

Martin Leinweber leads digital asset research and strategy at MarketVector Indexes, where he develops index products, publishes institutional research, and serves as the firm's primary voice on crypto markets to a global client base. His work sits at the intersection of systematic investing and an emerging asset class, translating rigorous quantitative frameworks into actionable insight for institutional investors.

Before joining MarketVector, Martin spent nearly two decades as a Portfolio Manager across equities, fixed income, and alternative investments. At Quoniam Asset Management, one of Germany's foremost quantitative houses, he managed active funds for institutional clients including insurance companies, pension funds, and sovereign wealth funds. Earlier in his career at MEAG, the asset manager of Munich Re and ERGO, he contributed to the firm's international expansion, including the establishment of a joint venture with PICC, China's largest insurance company, with operations in Shanghai and Beijing.

Martin is co-author of two Wiley publications: Asset-Allokation mit Kryptoassets: Das Handbuch (2021), the first institutional handbook on integrating digital assets into traditional portfolios, and Mastering Crypto Assets: Investing in Bitcoin, Ethereum, and Beyond (2024). He holds a Master of Economics from the University of Hohenheim and is a CFA Charterholder.

IMPORTANT DEFINITIONS AND DISCLOSURES

It is not possible to invest directly in an index. Exposure to an asset class represented by an index is available through investable instruments based on that index. MarketVector does not sponsor, endorse, sell, promote, or manage any investment fund or other investment vehicle that is offered by third parties and that seeks to provide an investment return based on the performance of any index. MarketVector makes no assurance that investment products based on the index will accurately track index performance or provide positive investment returns. MarketVector is not an investment advisor, and it makes no representation regarding the advisability of investing in any such investment fund or other investment vehicle. A decision to invest in any such investment fund or other investment vehicle should not be made in reliance on any of the statements set forth in this document.

Investments into cryptocurrencies and/or digital assets are subject to material and high risk including the risk of total loss. The calculated prices may not be achieved by investors as the calculated price is based on prices from different trading platforms. Furthermore, an investment into cryptocurrencies and/or digital assets may become illiquid depending on the trading platform or investment product used for the specific investment. Investors should carefully review all risk factors disclosed by the relevant trading platform or in the product documents of relevant investment products.

Prospective investors are advised to make an investment in any such fund or other vehicle only after carefully considering the risks associated with investing in such funds, as detailed in an offering memorandum or similar document that is prepared by or on behalf of the issuer of the investment fund or other vehicle. The inclusion of a security within an index is not a recommendation by MarketVector to buy, sell, or hold such security, nor is it considered to be investment advice.

All information shown prior to the index launch date is simulated performance data created from backtesting ("Simulated past performance"). Simulated past performance is not actual but hypothetical performance based on the same or fundamentally the same methodology that was in effect when the index was launched. Simulated past performance may materially differ from the actual performance. Actual or simulated past performance is no guarantee for future results.

ENDNOTES

[i] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS)*, Santa Fe, NM, November 20–22, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.
[ii] Google Quantum AI (March 2026). This whitepaper demonstrated a 20-fold reduction in required qubits (down from prior estimates of over 10 million) for solving the elliptic curve discrete logarithm problem (ECDLP) on the secp256k1 curve via advanced algorithmic optimizations

[iii] BIP-360, co-authored by Hunter Beast, introduces a Pay-to-Merkle-Root (P2MR) output type (initially designated P2QRH). This protects Taproot-native addresses from long-exposure quantum attacks while preserving scripting functionality for layer-2 scaling solutions like the Lightning Network.
[iv] These refer to the finalized post-quantum cryptographic standards approved by the National Institute of Standards and Technology (NIST) to replace legacy algorithms that are vulnerable to quantum decryption.
[v] The Hourglass V2 proposal mathematically extends the time required to drain quantum-vulnerable Pay-to-Public-Key (P2PK) addresses to over 32 years. This is specifically designed to mitigate the market impact of a sudden quantum theft of early dormant coins, such as Satoshi Nakamoto's estimated 1.1 million BTC.

[vi] Lopp, J. "Post-Quantum Migration and Legacy Signature Sunset." This proposal disallows new spends to quantum-vulnerable script types to force a network upgrade, effectively sunsetting legacy ECDSA and Schnorr signatures while minimizing the future attack surface.
[vii] EIP-7702 structurally advanced Ethereum's quantum readiness by enabling native account abstraction. This allows for incremental, per-wallet migration to arbitrary post-quantum signatures without requiring network-wide hard forks.