Bitcoin And Quantum Computing

Published: March 11, 2026

Author: Dhruv Bansal,
Co-Founder and CSO
at Unchained

Author: Tom Honzik,
Director of Custody Research
at Unchained

Author: David Puell,
Research Trading Analyst/
Associate Portfolio Manager,
Digital Assets at ARK Invest

Join the conversation on X
@ARKinvest @unchained

www.ark-invest.com
www.unchained.com

ARK INVEST | Unchained

Table Of Contents

Introduction

This paper assesses whether and how advances in quantum computing (QC) pose a risk to Bitcoin. Our two central arguments are as follows:

1. Quantum is a long-term risk but not an imminent threat. The community must continue to research and make plans for protecting the network as quantum computers improve.
2. If quantum computing were to affect Bitcoin's cryptography, the process would be protracted and undertaken at meaningful cost to the attacker.

Today's quantum systems lack the capabilities required to compromise Bitcoin. Meaningful breakthroughs would disrupt internet security first, triggering coordinated responses well beyond Bitcoin. In our view, quantum development will be a gradual technological progression—not a sudden "Q-day" event—giving markets and the Bitcoin network time to adapt.

Quantum computers use qubits that can exist in superposition, enabling quantum algorithms to scale more quickly than classical algorithms. Their performance is measured by parameters like the number of logical qubits and the degree of logical depth, both of which must be high and error-corrected to have an impact on Bitcoin. Today's systems operate in the so-called "NISQ era"—roughly 100 logical qubits and circuit depths in the hundreds—both well below the thresholds necessary to break Bitcoin's elliptic curve cryptography (ECC). To do so would require at least 2,330 logical qubits and tens of millions to billions of quantum gates.

Of the Bitcoin supply currently exposed to the quantum threat, ~1.7 million bitcoin (BTC) lie in vulnerable P2PK address types and are believed to be lost, and ~5.2 million BTC lie in migratable re-used or P2TR addresses—adding to ~35% of total outstanding supply.[1]

That said, quantum risk is unlikely to surface as an event but as a protracted sequence of observable milestones, as follows:

- ***Stage 0:*** Quantum computers exist but are not commercially useful. Today's quantum computers operate with limited logical qubits and high error rates, presenting no threat to Bitcoin.
- ***Stage 1:*** Quantum computers become commercially useful in fields like chemistry and materials simulation, well before cryptographic applications manifest.
- ***Stage 2:*** Quantum computing becomes powerful enough to break weak keys or deprecated cryptosystems.
- ***Stage 3:*** Quantum computers can break elliptic curve cryptography of the kind used for bitcoin keys, but they take a long time to do so. Quantum-vulnerable bitcoin is now at risk.
- ***Stage 4:*** Key-breaking occurs more quickly than Bitcoin's 10-minute block time, network viability requiring protocol-level, post-quantum cryptography upgrades.

Against that backdrop, the most important investment-related questions are:

- When will quantum computing break an elliptic curve key for the first time, and when will the subsequent break take place?
- Who will control early quantum capability, and what will be their incentives?
- What will quantum attacks cost relative to other more profitable or rewarding efforts?
- How effectively will the Bitcoin community coordinate governance decisions and implement post-quantum cryptography?

This paper argues that quantum risk will evolve over an extended period of time, with many intermediate warning signals and decision points. An abrupt single point of failure is unlikely.

The Basics

In 2010, Satoshi Nakamoto addressed early concerns about the quantum computing threat, as shown below.

From: satoshi
Subject: **Re: Major Meltdown**
Date: July 10, 2010 at 13:36:17 UTC

> **Quote from: llama on July 01, 2010, 10:21:47 PM**
>
> However, if something happened and the signatures were compromised (perhaps integer factorization is solved, quantum computers?), then even agreeing upon the last valid block would be worthless.

True, if it happened suddenly. If it happens gradually, we can still transition to something stronger. When you run the upgraded software for the first time, it would re-sign all your money with the new stronger signature algorithm. (by creating a transaction sending the money to yourself with the stronger sig)

Source: Nakamoto Institute 2026.[2] For informational purposes only and should not be considered investment advice or a recommendation to buy, sell, or hold any particular security or cryptocurrency.

Today, industry participants continue to debate the threat. While perspectives differ with respect to timeline and likelihood, recent commentary appears to be coalescing around a neutral view: quantum computing represents an actionable long-term issue—not an immediate security emergency—and requires preparation.

Many have sprung into action. Coinbase has established its Independent Advisory Board on Quantum Computing,[3] for example, offering guidance on quantum threats to the broader digital asset community. The Ethereum Foundation has its Post Quantum (PQ) team,[4] tasked to prepare the Ethereum network for quantum computing viability. Strategy (formerly MicroStrategy) will initiate its Bitcoin Security Program[5] to "coordinate with the global cyber, crypto, and Bitcoin security communities" and tackle the quantum computing threat. Bitcoin Improvement Proposal (BIP) 360—a proposal supporting a new output type called Pay-to-Merkle-Root (P2MR), designed to address Taproot's quantum vulnerabilities—has just been updated and merged into Bitcoin Improvement Proposal (BIP) GitHub repository.

These initiatives signal that ecosystem players take quantum resilience seriously as a feature of their companies' long-term risk management practices.

Quantum Computing

Quantum computers and classical computers process information in very different ways. Whereas classical computers operate on bits—representing either a 0 or a 1 state—quantum computers use qubits, which can exist in superposition of both the 0 and 1 states simultaneously, enabling some algorithms to solve specific problems, sometimes exponentially faster than classical approaches.

Measures of performance rely on benchmarks like number of logical qubits (error-corrected qubits capable of sustained computation) and logical gate depth (how many operations can be executed reliably before errors accumulate).

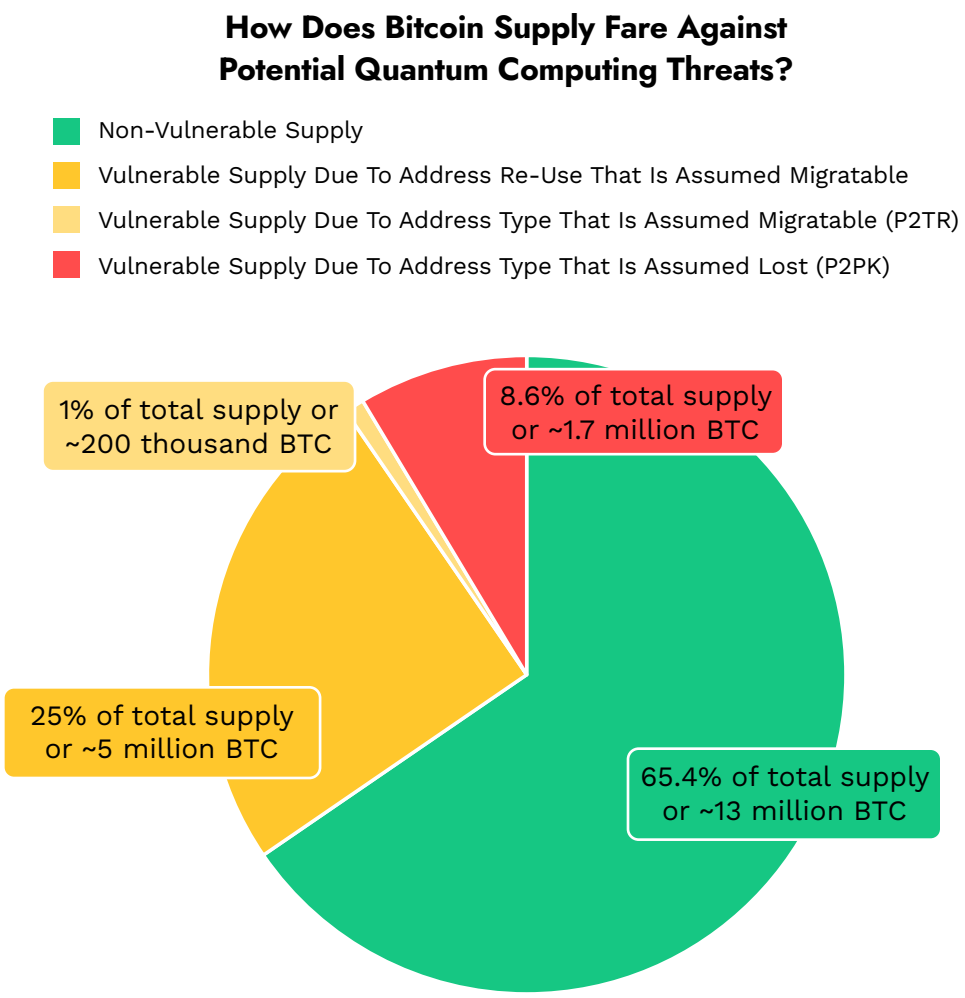
Importantly, today's quantum systems remain far below the thresholds required to break modern cryptography. That said, Shor's algorithm—one of the key theoretical constructs driving concerns about a threat—demonstrates that sufficiently powerful quantum computers could solve some of the number-theoretic problems that underpin widely used public-key cryptography across all digital infrastructure.

To be sure, quantum computing does pose a security risk, not only to Bitcoin but to all digital infrastructure based on cryptographic assumptions—from internet encryption and cloud infrastructure to banking systems and government communications. As a result, any quantum breakthrough capable of undermining such systems would have broad, economy-wide implications. In other words, the incentive to prepare extends far beyond the Bitcoin community.

Bitcoin Cryptography

Bitcoin's security model relies on two primary cryptographic mechanisms. "Hash functions" secure mining, block linking, and transaction ordering, while "elliptic curve cryptography" (specifically ECDSA over the secp256k1 curve) uses digital signatures to secure ownership and spending.

Current research suggests that hash functions are more resistant to quantum attacks,[6] while breaking elliptic curves would put ~1.7 million BTC in "quantum-vulnerable" addresses assumed lost—as well as another ~5.2 million vulnerable BTC that could be moved to quantum-secure addresses—at risk of potential theft over a period of time,[7] as shown below. If breaking ECC could be done within a few minutes, then transacting with bitcoin in quantum-protected addresses also will be vulnerable to theft.



Source: Unchained and ARK Investment Management LLC, 2026, based on data from Project Eleven 2026. For informational purposes only and should not be considered investment advice or a recommendation to buy, sell, or hold any particular security or cryptocurrency.

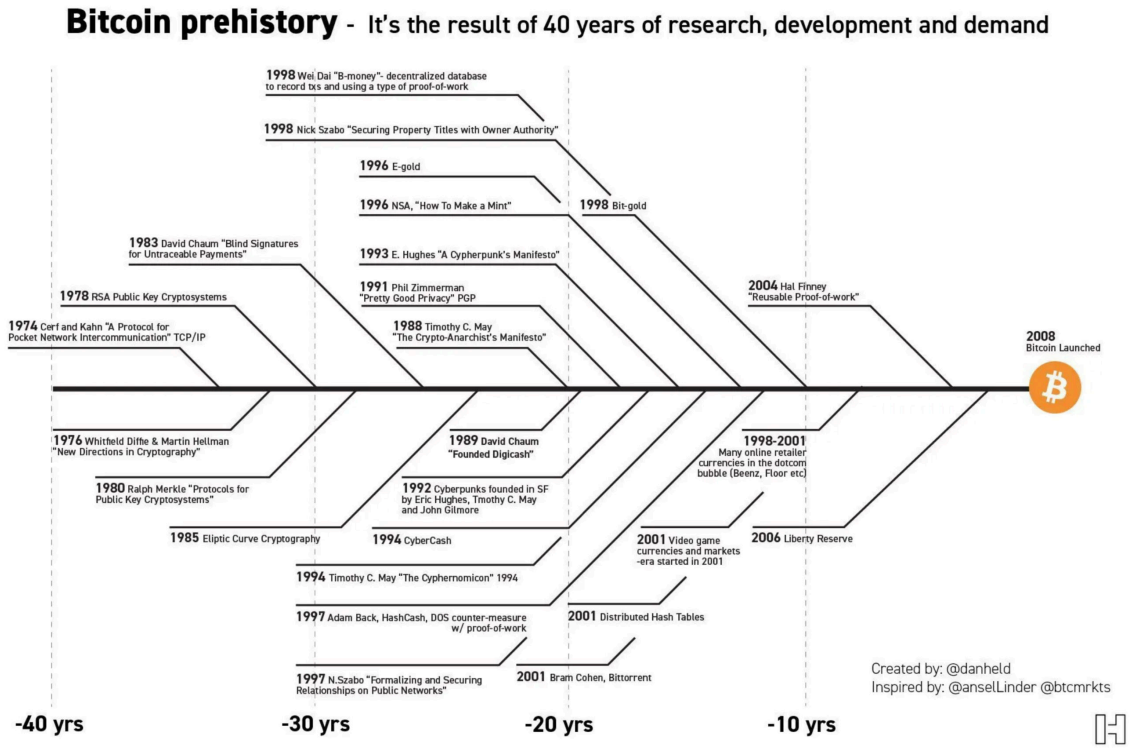
Even so, their practical feasibility would require quantum systems to reach performance levels that our research suggests will take much time to achieve.[8] If quantum progress follows current projections, how likely is it to meaningfully disrupt Bitcoin's usage, security model, or value proposition? Framed thusly, investors should be focused on the timelines of evolving technological change and the robustness of decentralized systems as that change unfolds.

Quantum Computing Capability Is A Journey

Commentators often parse two distinct eras in the development of quantum computing in relation to Bitcoin: one era in which quantum computing cannot affect Bitcoin and another in which it has broken Bitcoin's underlying cryptography completely. That framing implies a bifurcation, a sudden, catastrophic moment marking the transition from one era to the next—a "Q-day" event that will happen at some specific time in the future whose timing remains unknown.

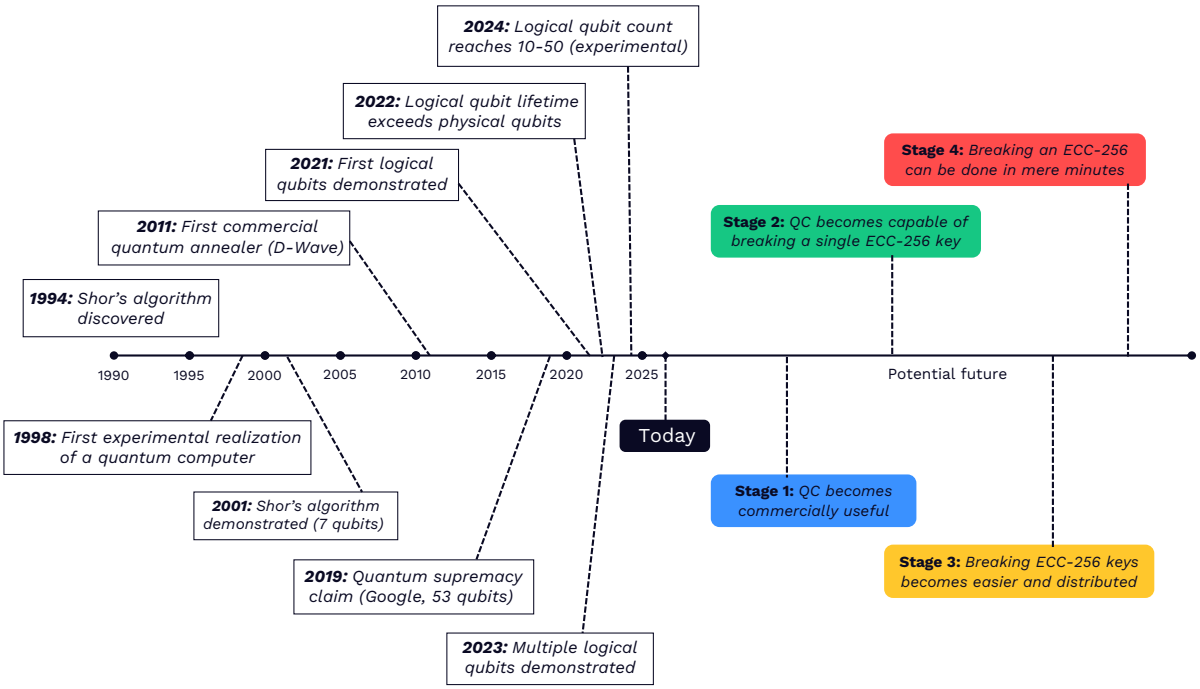
Unfortunately, bifurcation turns out to be crude in this case. For example, the technology stack enabling our global network of internet-connected smartphones wasn't invented on any particular date. Instead, technologies mature through the compounding of small improvements and occasional major breakthroughs. Each advance creates the conditions of possibility for other events to unfold, sometimes making the technology more useful, less expensive to produce, more profitable to manufacture and sell, and worthy of further investment.

Even Bitcoin is the result of at least 40 years of ongoing research and development in cryptography, peer-to-peer networks, and digital currencies, as illustrated below.



Source: The Cypherpunks/Held 2018.[9] For informational purposes only and should not be considered investment advice or a recommendation to buy, sell, or hold any particular security or cryptocurrency.

The development of quantum computing, including its potential impact on Bitcoin, should unfold like the development of other transformative technologies—a long-term process entailing numerous intermediate events and contingencies, as shown below.

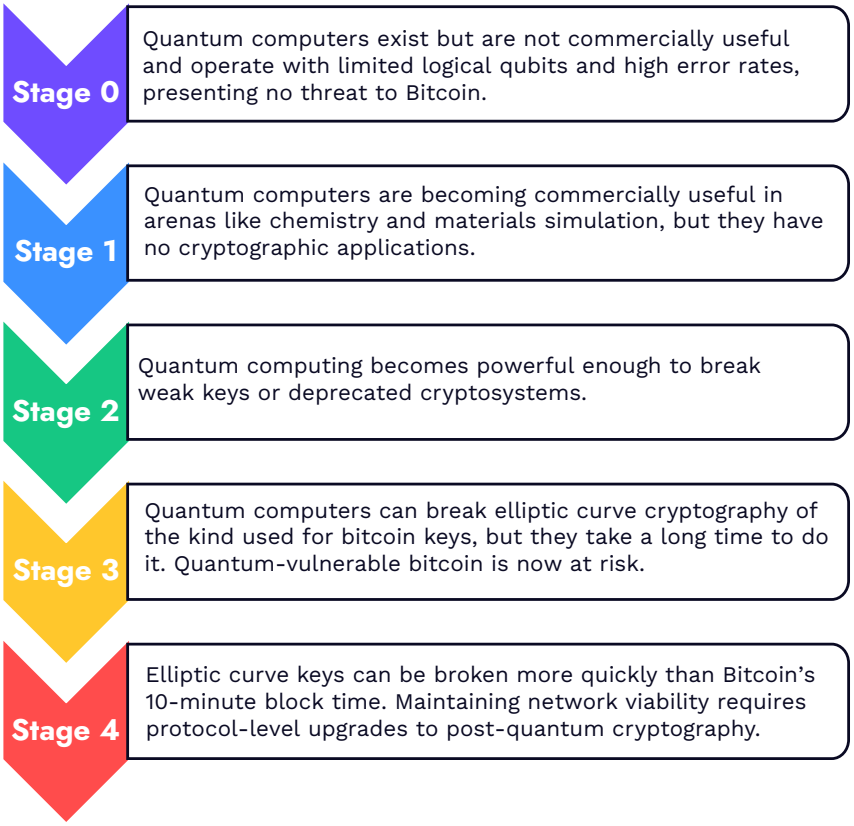


Source: Unchained and ARK Investment Management LLC, 2026, based on data collated in Quantum Computing Timeline/GitHub. [https://ddri.github.io/] as of February 2, 2026. For informational purposes only and should not be considered investment advice or a recommendation to buy, sell, or hold any particular security or cryptocurrency.

Understanding the security and reliability of bitcoin as a long-term store of value requires us to appreciate that quantum computing will develop over years, if not decades, through an ongoing process of intermediate events.

Importantly, so will its impacts on Bitcoin. Indeed, what we call "risk" unfolds similarly to what we call "progress" or "advancement"—incremental events that create the conditions for others, all compounding toward some outcome. Fortunately, the Bitcoin community is taking the risk of quantum computing seriously, before its most potentially problematic outcomes unfold, giving investors and bitcoin holders the opportunity to monitor the development of quantum computing, updating predictions in response to the industry's accelerated or delayed achievement of various milestones along the way. A case in point, the BIP 360 proposal has just been published on the Bitcoin Improvement Proposal (BIP) GitHub repository, with aims to make Taproot addresses quantum-resistant, reducing attack risk while keeping Taproot's functionality intact.

As a result, we believe the most productive approach is to construct a high-level timeline of potential stages in the advancement of quantum computing, explicating how each stage could impact Bitcoin, as shown below.



Source: Unchained and ARK Investment Management LLC, 2026. For informational purposes only and should not be considered investment advice or a recommendation to buy, sell, or hold any particular security or cryptocurrency.

Stage 0: Quantum Computers Exist But Are Not Commercially Viable

In the early 1980s, the physicist Richard Feynman speculated that a "quantum computer" would be best at simulating quantum systems. While theoretical work advanced during the next decades, only by the turn of the century were researchers able to build successful quantum computers. Several hundred quantum computers now exist in research labs around the world, though they are not commercially viable.

Quantum computing researcher John Preskill characterizes today's quantum technology as the "Noisy Intermediate-Scale Quantum" (NISQ) era. Leading demonstrations have achieved up to nearly 100 logical qubits, hundreds of logical operations, and a logical depth of ~65, with varying levels of error correction. Those figures vary significantly based on hardware platform, error-correction methods, and experimental conditions, however, making direct comparisons challenging.[10]

Quantum computers' most useful capability in the NISQ era is performing reflexive experiments that help researchers understand quantum computing. Indeed, contemporary classical computers remain superior to quantum computers for all truly useful, commercially viable applications. As a result, investment in quantum computing has yet to yield financial returns, and no profitable quantum computing startups or businesses currently exist. Belief in its potential currently drives all public and private investment.

The bulk of quantum computing research and development occurs in the geopolitical regions with most funding, infrastructure, and knowledge—North America, Europe, and China. In the West, a mix of private and public companies lead the way, each with its own mix of funding from venture capitalists, government grants, or Big Tech research and development (R&D) reserves, including those of Google, IBM, Microsoft, Quantinuum, IonQ, PsiQuantum, Alice and Bob, and QuEra, among others,[11] whose breakthroughs are shared in public reports. In China, quantum computing takes a more government-led approach, with some research recently transitioning from major tech firms like Baidu and Alibaba to state-run university programs.[12]

Stage 0 Historical Milestones:

- First experimental realization of a quantum gate (1995).[13]
- First experimental realization of a quantum computer (1998).[14]
- First experimental realization of error correction (1998).[15]
- First experimental realization of Shor's algorithm for factoring and discrete log problem (2001).[16]
- Total historical capital invested into quantum computing (~$60 billion).[17]

Stage 1: Quantum Computers Are Commercially Viable

In the early 1980's, Feynman was thinking about quantum computing in relation to the possibilities for simulating physics—the interactions between atoms and molecules and light—not in relation to breaking cryptography. That preoccupation continues to dominate the mindshare of most quantum computing researchers and investors, because simulating small, real-world quantum mechanical systems continues to be the most valuable near-term application. It also turns out to be much easier than building a quantum computer that can break modern cryptosystems, which requires vast capabilities.

For example, a reliable, fault-tolerant quantum computer with a modest ~100 logical qubits, a circuit depth of 10^3-10^6 and 10^5-10^7 two-qubit gates would become useful for new research in a variety of fields like chemistry.[18] The U.S. Defense Advanced Research Projects Agency's (DARPA's) Quantum Benchmarking program has identified specific industrial priority targets, including homogeneous catalyst discovery (for fertilizer production), incompressible fluid dynamics (for aerospace and ship design), corrosion-

resistant materials, and binding affinity calculations (for drug discovery and biological processes like Alzheimer's research). Those proposals could revolutionize fields from battery catalysis and solar cell efficiency to financial risk modeling and nuclear fusion simulation.[19] Boston Consulting Group (BCG) refers to this stage—when quantum computers are better than classical computers at some specific, high-value use cases—as "Broad Quantum Advantage."[20]

Instead of providing an estimate of when quantum computing will achieve Stage 1, we identify milestones, as shown below, that can indicate the rate of progress toward and through Stage 1. Our research suggests that this stage will not affect bitcoin's price beyond short-term speculation.

Milestones:

- Quantum computers in research labs can perform computations reliably using ~100 logical qubits and a circuit depth of 10^3-10^6.
- These labs begin to publish useful research—not about quantum computing, but about progress in other fields.
- The cost and difficulty of manufacturing quantum computers at this scale is costly and difficult, so much so that the technology generally remains non-viable commercially.
- Even so, several companies begin to make profits from quantum computing by manufacturing and selling quantum computers.

Stage 2: Quantum Computers Can Break Weak Or Old Cryptography

Quantum computing researchers have begun to refer to the "Cryptographically (or Cryptoanalytically) Relevant Quantum Computer" (CRQC), a quantum computer that poses a threat to real-world cryptosystems.

But not all cryptosystems are the same. Before an advanced CRQC exists that can break the strong 256-bit ECC used by Bitcoin, a simpler CRQC will exist that can break weaker cryptosystems—those using shorter keys or buggy implementations, for example. As a result, CRQCs attacks are likely to begin on the most vulnerable systems, steadily working their way toward stronger systems like Bitcoin.

Current cryptographic standards and guidelines[21] recommend using cryptosystems as strong or stronger than Bitcoin's. Modern systems following those rules should be protected not only against classical computers but also against early-generation quantum computers.

Importantly, however, computing and the internet are decades-old and many living digital systems predate modern encryption standards. If quantum computing were to become powerful enough to threaten cryptography, attacks on weak keys and deprecated cryptosystems will become commonplace, especially if so-called “harvest now, decrypt later” intelligence agency and criminal organization practices exist.

Again, quantum computing might never scale to the extent required to deliver a CRQC; on the other hand, the science could accelerate very quickly beyond this stage to the more dangerous ones described below. That said, apart from associated market speculation, our research suggests that Stage 2 poses no threat to Bitcoin’s supply side.

Milestones:

- Historical data previously believed to be private are decrypted through a CRQC and leaked publicly for political or financial gain.
- The rate at which denial-of-service (DoS) and ransomware CRQCs attacks compromise weak systems increases.

Stage 3: Quantum Computers Can Break Bitcoin’s Cryptography, Though Slowly

Advances in quantum computing eventually will make Bitcoin vulnerable to a CRQC. Broadly, bitcoins are stored in two kinds of addresses: quantum-resistant and quantum-vulnerable. Broadly speaking, bitcoin deposits created before 2011 tend to be quantum-vulnerable—given the address type widely used at the time, P2PK—while more recent systems tend to be quantum-resistant.[22] The good news is that bitcoin holders can use quantum-resistant addresses across a broad range of wallets and custodians, a possibility detailed in an article by the team at Unchained.[23]

That said, a CRQC able to break Bitcoin’s cryptography will put bitcoins stored in quantum-vulnerable addresses at risk. Estimates suggest that up to ~1.7 million BTC could be affected, excluding currently-vulnerable coins that are not lost and therefore could be transferred to quantum-resistant addresses, which amounts to ~5.2 million BTC.[24]

But a quantum computer can attack only one vulnerable address or public key at a time, so a CRQC attacker will still not be able to steal the full balance of quantum-vulnerable addresses all at once. An important unknown, therefore, is the amount of time it would take for a CRQC to break a single ECC public key. The longer that takes, the more time attackers need to steal the full balance of quantum-vulnerable coins. If quantum computers reach this stage, part of Bitcoin’s supply could come back to circulation and increase its supply side, albeit at a slow, diminished rate based on the cost to attack individual keys.

Milestones:

- A quantum computer exists that has thousands of logical qubits,[25] millions to billions of gates, and a circuit depth of up to ~10^{11} sequential operations—a CRQC.[26]
- This CRQC is used to break a 256-bit ECC public key.
- The first attacker uses the CRQC to steal bitcoin from a quantum-vulnerable address, likely the address that holds the highest bitcoin balance.
- Such attacks continue and accelerate over time as the technology improves.

Stage 4: Quantum Computers Can Break Bitcoin's Cryptography, Quickly
If the time taken to execute a successful quantum attack on an ECC public key becomes extremely short—a few minutes or less—then the full balance of quantum-vulnerable coins could be stolen within days or weeks.

Even worse, bitcoin stored in quantum-resistant addresses also will become vulnerable as soon as it is moved. Bitcoin blocks are produced approximately every ten minutes, and so a CRQC that breaks ECC more quickly than that poses a danger, because it can attack any pending transactions visible in the public Bitcoin mempool. Even users following best practices and using quantum-resistant addresses become vulnerable to losing funds.

Inaction at the protocol level during Stage 4 would threaten Bitcoin as a useful monetary system in quite serious ways—an existential threat to the protocol. For Bitcoin to operate as a functioning currency, it must support entirely quantum-safe addresses before quantum computing develops to Stage 4.

Fortunately, a proposal for quantum-safe Bitcoin addresses already exists,[27] and the people and industries investing in bitcoin are highly incentivized to ensure a solution.

Important Questions For Investors

Many caveats apply to our simplified, hypothetical framework. Instead of being completely distinct, for example, stages 0-4 could overlap in important ways. Our purpose in offering these stages is to demonstrate that the threat model of quantum computing affecting Bitcoin looks more like a journey than a single Q-day event.

Against that backdrop, we believe investors should be asking specific questions that should help to clarify the timing of events, the speed of progression, the entities involved, and the mitigations and protections that might guard against threat. The process of asking questions and finding answers can create conviction in one's choice either to invest in and hold bitcoin or to sell it to a willing buyer. Prudent investors will revisit these questions over time.

How long until the first Bitcoin public key is broken?

Some worry that major quantum breakthroughs will create a CRQC capable of attacking Bitcoin before 2030,[28] while others suggest that CRQCs are decades away.[29] Between those views lie the institutional projections both from companies developing quantum computing development—e.g., Google, IBM, Microsoft—and government agencies like the National Institute of Standards and Technology (NIST). These entities share a consensus target in the mid-2030s.[30]

A minority viewpoint suggests that practical quantum computing is a fantasy on any timeline,[31] which we believe could underestimate human inventiveness and underestimates the growing human need for quantum computing. The capabilities of classical electronic computers improved by approximately ten to fifteen orders of magnitude over the course of 80 years.[32] If quantum computing were to repeat that pattern over the next 80 years, we will have passed through all five stages of our timeline. We believe that stringent skepticism around quantum computing is based on an immune response to the industrialized hype surrounding certain quantum computing companies' possibly disingenuous claims. Ironically, some quantum computing researchers might agree.[33]

How long until the second Bitcoin public key is broken?

Equally crucial, some wonder how much time will pass between the break of the first and second public keys. Some commentators assume that the break of the first key will lead to a cascade of further immediate keys breaks, as if breaking keys using a CRQC requires minimal time and resources—akin to sending emails or signing bitcoin transactions. As argued above, if a CRQC exists that can break a Bitcoin private key extremely quickly, then we are already in Stage 4.

A plausible alternative is that breaking the first 256-bit ECC public key is a massive effort that cannot be replicated easily until other major capabilities are developed. We view that situation as especially likely, since breakthroughs in the capabilities and scale of a technology typically happen first in research labs then develop and scale over time.

A slow, protracted breakage of Bitcoin public keys would mitigate impact on the network to some extent. For example, the ~1.1 million BTC believed to be mined by Satoshi are spread out across ~22,000 different quantum-vulnerable addresses, each protecting 50 BTC. If the operator of a quantum computer wants to take those coins, they must break each public key separately. If breaking a single public key takes one hour, the process would take more than three years. If breaking a single public key takes a day, then it will take 60 years, if a week, then more than 400 years.

If numerous attackers operated quantum computers of similar capability concurrently, the timeline would shorten. As technology advances, the duration of each attack should compress, further accelerating the timeline. But we believe various combinations—of

required attack duration, rate of technology improvement, number of attackers, and cost of attack—imply that the global theft of all quantum-vulnerable coins could take several years.

Who will be able and motivated to break public Bitcoin keys?

Today's quantum computers exist only in research labs and are unlikely to be used to commit crimes. They are operated by major institutions with significant reputations to lose and are essentially useless. But who will have access to quantum computers as the timeline advances?

The history of AI is instructive, since it illustrates one way to think about the answer. Fictional depictions suggesting that a single person or company invented an all-powerful AI capability that had big consequences seem silly now that AI is everywhere advancing on multiple fronts. Countless AI companies now compete to advance the technology.

The idea that an advanced CRQC will be built by a single entity that gains massive advantage should ring silly for the same reasons. If quantum computing ever advances by the orders of magnitude required to break Bitcoin keys, we believe that it already will have become a sprawling global industry comprising the efforts of countless companies finding ways to profit from all the useful things quantum computers can do by simulating nature. In other words, quantum computers of varying capabilities will be distributed across the globe. Cloud services that democratize access to quantum computing by allowing people with classical computers to define calculations to run on remote quantum computing clusters also will exist (such services already exist today in our NISQ area). In that context, if some entity becomes the first to develop a CRQC that can break a Bitcoin public key, many other entities are likely only months away from replicating those achievements, and the general public only a year away from obtaining remote access.

As a result, the ability to steal bitcoin could be widespread, much like using AI to scam people and commit other crimes. As with AI, people's willingness to use quantum computers to commit crimes will be influenced by the ease and cost of mounting the attack and the likelihood of success.

What will it cost to break Bitcoin public keys?

A Bitcoin attacker will be motivated[34] by profit, and the market value of any stolen bitcoin must be compared against the cost incurred while breaking a key. In Stage 3, breaking the first 256-bit Bitcoin ECC key likely will involve running one of the most advanced quantum computers in the world for a significant length of time, its cost non-trivial.[35] Such a powerful system not only consumes substantial energy for cryogenic cooling and control electronics, but also incurs significant development, manufacturing, operations, staffing, and maintenance costs.

Manufacturing costs are difficult to calculate at this stage, but The Homeland Security Operational Analysis Center estimated in 2023 that breaking one public key would incur electricity costs of ~$100,000. The bad news for bitcoin holders? The cost of quantum computation is likely to fall, while the value of bitcoin is likely to increase. As a result, the costs to would-be Bitcoin CRQC attackers is likely to decrease over time, and so will cost as a mode of defense.

How can we protect Bitcoin from quantum computing?
The good news is that we already know how to protect against quantum attacks. The majority of Bitcoin's supply is held in quantum-resistant addresses, and the remainder is held in quantum-vulnerable addresses that should not be at risk until Stage 3 of our timeline, when a CRQC exists that can break a 256-bit ECC key.

But to be truly free from all quantum computing risk—even in Stage 4, when CRQCs are fast enough to pose a risk to bitcoin in quantum-resistant addresses—Bitcoin must implement some kind of quantum-safe address format, which will require integrating some form of post-quantum cryptography (PQC) into Bitcoin.

PQC Is Widely Deployed

Defense against quantum computers through post-quantum cryptography (PQC) already exceeds progress in building CRQCs. We are still in Stage 0, NISQ, when quantum computers are essentially useless and CRQCs do not exist, while several promising post-quantum cryptosystems have been invented and deployed across the internet.

Indeed, PQC research has been ongoing ever since the discovery of Shor's algorithm. Two associated signature schemes have been tested rigorously by NIST and were standardized in 2024[36]: ML-DSA, which uses lattice-based signatures,[37] and SLH-DSA, which uses hash-based signatures.[38] Those standards give us confidence in the capabilities of post-quantum cryptography. Warnings issued by recent versions of OpenSSH—when forced to use a quantum-vulnerable encryption protocol while making a connection to a server that doesn't support PQC—are shown below.

```
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
```

The computer security world is integrating these standards into the software backbones of the internet. Recent versions of communication protocols like OpenSSH and OpenSSL ship with PQC as the default, some of which already emit warnings when making purely classical connections.[39] Web infrastructure providers from browsers to

content delivery networks (CDNs) have integrated PQC, and significant portions of global Internet traffic are already quantum-safe. You may be reading this article through a quantum-safe communication channel!

Implementing PQC In Bitcoin Will Require Consensus Changes

Upgrading the Bitcoin network to use PQC at the consensus level that governs transactions will be more difficult, given additional constraints on Bitcoin that are not present in more traditional internet applications, as follows:

- Storing data in the blockchain and computing inside the Bitcoin Script virtual machine is expensive and constrained by consensus limits, which forces PQC implementation to be more efficient with data and compute resources.
- The PQC implementation should be easy to integrate with existing custody practices, tools like hierarchical deterministic (HD) wallets, and hardware devices available in the market.
- Consensus changes, including those that require only soft forks, historically have created tension, conflict, and division within Bitcoin's decentralized developer community, miners, and investors.

For those reasons, no proposed PQC implementation (e.g., BIP 360) has emerged as a consensus choice.[40] Each proposal comes with various tradeoffs like speed, complexity, key size, signature size, and statefulness. In December 2025, Blockstream Research published an analysis of hash-based signatures, noting that they are particularly compelling because Bitcoin already relies on the efficacy of hash functions,[41] sparking ongoing discussions around statefulness tradeoffs and further optimization.[42]

We have described the risks of inaction, but risks also come with moving too quickly. Bitcoin is not OpenSSH, a privately managed computer network, or even an altcoin where deployed versions can be updated easily and rolled back if bugs or bad performance are encountered. Deploying PQC into Bitcoin is difficult, because changes of any kind to its consensus layer are challenging by design. Bitcoin moves slowly and may incorporate only a handful of consensus changes over its entire lifetime—a dynamic known as ossification. Integrating a hastily reviewed PQC implementation that introduces bugs, or that compromises some other aspects of Bitcoin's functionality, would be a setback and require further fixes.

That said, if enough of the Bitcoin ecosystem can agree on a PQC implementation, then a soft fork that provides a new kind of quantum-safe Bitcoin address could become a

reality. The Bitcoin ecosystem's timeline for achieving that depends on one's estimate of the time it takes the quantum computing industry to reach Stage 3 and 4 of our timeline.

No Consensus Exists About Protecting Coins That Remain Vulnerable To Quantum

If Bitcoin develops a truly quantum-safe PQC address implementation, bitcoin holders are likely to migrate their holdings to the new format, either slowly or quickly, depending on their level of concern.

Even so, a large balance of bitcoins in quantum-vulnerable addresses—in other words, bitcoins considered lost or abandoned and not migratable—will remain. Such bitcoins are likely to be stolen by capable CRQCs.

Some commentators propose preventing the theft of those coins through additional consensus changes to Bitcoin that would lock—"freeze" or "burn"—old, quantum-vulnerable coins permanently. In that case, a notice would be issued in advance, so that the owners of quantum-vulnerable coins can move them to safety.

But at some point, remaining quantum-vulnerable coins would not be able to be transferred or sold by anyone, even if their original owners (presumed absent) were to try. Proponents of this idea claim that freezing vulnerable coins, thereby diminishing Bitcoin's supply permanently, would be better for Bitcoin than were those coins to be stolen by an attacker. In both cases, the previous owners will have lost their coins, and the attackers would not be able to acquire them.[43]

Critics argue that preventing bitcoin from being spent "by fiat" would set a dangerous censorship precedent under the guise of safety(ism).[44] Bitcoin is a disruptive, new kind of money, in part because it gives its holders direct, self-sovereign, unalienable control with no counterparty risk. The cost of that control is personal responsibility, committing to protect one's own private keys without expecting the network, a custodian, or a bank to do so on one's behalf. In this view, doing nothing is simplest and aligns best with the Bitcoin community's ethos of self-reliance and decentralization.

We believe that choosing how to implement PQC and deploy it on-chain should remain decoupled from the question of what to do about coins that remain quantum-vulnerable. Yet the two matters often are conflated, the controversy around the latter often clouding discussions of the former.

Three Scenarios

Without perfect answers to the crucial questions laid out above, predicting outcomes is ill-advised. Instead, we find it useful to sketch a range of plausible scenarios—pessimistic, optimistic, and balanced, as detailed below. The scenarios are constructed mostly with respect to quantum computing's impact on Bitcoin; thus, our pessimistic scenario is pessimistic for Bitcoin, hence optimistic for quantum computing—and vice versa.

Plausible Pessimistic Scenario

The most plausible pessimistic scenario entails a sudden breakthrough in quantum computing, perhaps powered by next-generation artificial intelligence, that causes the quantum computing industry to jump more quickly and in unexpected ways to a much later stage in our timeline. Both the Bitcoin ecosystem and the broad global computer security ecosystem would be underprepared. Bitcoin developers would have to scramble for a quick solution with little time for careful consideration.

Even in the pessimistic scenario, we believe Bitcoin will continue to function and that most bitcoin holdings will be safe. PQC proposals for Bitcoin already exist. They are not being incorporated yet, because we do not have consensus that they are the right choices or that now is the right time. In a world in which CRQCs have verifiably arrived, are widely understood to have the capacity to attack Bitcoin, or are already attacking it, PQC proposals will be implemented swiftly and pushed out to the network. If attackers can use AI to build CRQCs, then defenders can use AI to integrate PQC. No single body, such as Bitcoin Core, is required. Anyone can update Bitcoin's software and distribute it and, in a time of potential chaos and uncertainty, the market is likely to cohere around whatever soft or hard fork of Bitcoin doesn't get hacked, regardless of its source.

Put differently, the amount of time that Bitcoin would lack quantum-safe addresses while a CRQC exists in the wild could be made short. The shorter that time, the less likely CRQCs will fall into the hands of attackers, the less time those attackers will have to mount attacks.

The cost of moving quickly is that the PQC fork that wins out after such a sudden fracas might not be optimal but present major tradeoffs for Bitcoin users, such as needing new hardware devices or new wallet software. Companies that provide Bitcoin financial and custody services could be impacted until they can convert their systems. Over time, bugs, technical debt, and security issues could require further changes.

Controversy around proposed solutions also could spawn a heated political conflict, where developers, thought leaders, Bitcoin users, and miners become antagonistic

toward one another. That would distract from finding a solution and cause further concern for some investors. Previous divisive proposals for Bitcoin development have led to unnecessary hard-forks and Bitcoin's split into two different coins.[45] Investors who take a side by trading one coin for another could lose substantial capital. Controversy over the least-worst, quantum-resistant signature scheme, or how to handle vulnerable "lost" coins, could escalate into a high-stakes scenario.

The sudden appearance of a CRQC would create chaos across many industries, not just Bitcoin: banking, financial services, social media, telecommunications, healthcare, and government would be in disarray as companies and technology providers scramble to protect themselves. The integrity of millions of ledgers and datasets that the world uses to keep itself in order would be called into question.

In that climate of uncertainty, Bitcoin could thrive. The proof-of-work that Bitcoin blocks chain together provide thermodynamic protection to Bitcoin's ledger that no quantum computer can subvert. As always, notwithstanding tumult, we believe Bitcoin will survive.

Plausible Optimistic Scenario

The plausible optimistic scenario is a partial inverse of the pessimistic one described above. Quantum computing development hits unexpected obstacles and fails to make expected progress. Analysts must re-revise their estimates out more decades. Investment slows and quantum computing enters its winter era—just as AI did, twice.

In this scenario, Bitcoin waits several decades for PQC research to advance. Developers needn't integrate quick and ill-considered choices and can use a trusted PQC algorithm that has been in use in other computing contexts for years. PQC could come to Bitcoin for reasons other than outrunning threats from quantum computers. For example, state-of-the-art PQC might be more efficient than the ECC that Bitcoin currently uses or provide powerful new capabilities like fully homomorphic encryption that enables significant increases in privacy.

Increased trust could facilitate consensus around a particular PQC proposal, giving the community time to agree about how to handle bitcoins that remain in quantum-vulnerable addresses. If agreement develops around a particular best path forward, then the resulting PQC soft fork will have a greater chance of entering consensus and cause minimal division and conflict in the Bitcoin community.

Once a strong PQC is available, Bitcoin users would have plenty of time to wait and upgrade into quantum-safe addresses. The hardware devices, wallets, and financial service providers that integrate with Bitcoin also would have time to adapt to the new address format. The realization that quantum risk is actively managed could create a tailwind for bitcoin investment.

Plausible Balanced Scenario

Between the optimistic and pessimistic scenarios is a balanced scenario that aligns with mainstream, institutional predictions about quantum computing progress. This scenario assumes that 10-20 years will pass before Stage 3, when a CRQC will be able to attack Bitcoin.

In our view, within 10-20 years the PQC research community will make enough progress on algorithms to give the Bitcoin developer community time to adapt and optimize them for the Bitcoin blockchain, virtual machine, and ecosystem of tools, devices, and companies.

Long before hitting Stage 3, the quantum computing industry is likely to become commercially useful in Stage 1, but CRQCs will take years. The existence of a viable and profitable quantum computing industry will increase the perception that CRQCs are a real risk, imbuing the Bitcoin community with a sense of urgency to rally around a PQC solution.

The network could release and adopt a PQC soft fork while in Stage 1, but multiple PQC proposals could split the community and create controversy, threatening the consensus around implementation. If the quantum computing industry were to enter Stage 2, Bitcoin users would have to consider evidence that CRQCs might be able to break weak keys and cryptosystems outside of Bitcoin, galvanizing its willingness to compromise and orchestrate a consensus.

That consensus choice could be flawed, with tradeoffs generating criticism for years. Nevertheless, in the balanced scenario, the community would implement quantum-safe addresses long before Stage 3, the time that CRQC might threaten bitcoin.

The default situation surrounding lost vulnerable coins is that no consensus changes freeze them or restrict their movement. Whether that remains the case or a consensus change does occur, there is likely to be some level of conflict between investors who are concerned about potential sell pressure from the gradual quantum-recovery of lost coins, and other users who are motivated to uphold alternative principles. While not everyone will be happy with either outcome, the supply limit of 21 million that supports the long-term investment thesis of many bitcoin holders remains intact. Controversy and conflict around the transition could hurt the price of bitcoin, but investors who understand the importance of a quantum-safe bitcoin could use the volatility as a buying opportunity.

The Road Ahead

Instead of framing quantum computing as an imminent threat, investors should focus during the next few years on insuring that Bitcoin and its underlying supply become quantum resistant, with concise governance decisions, responsible code-level modifications, and the migration of unsecured coins into secured wallets. As important as the eventual protocol-level response is educating investors—not only about quantum computing's impact on short-term market volatility, but also about the governance consensus and the adoption of post-quantum practices and infrastructure.

Investors should remain informed about the distinction between theoretical quantum risks and practical solutions. Market volatility often arises in response not only to fundamentals but also to misperceptions. As quantum computing evolves either slowly or rapidly, digital asset price volatility could reflect uncertainty more the fundamental security of Bitcoin and other digital assets.

Most major digital and other financial assets with an established track record rely on cryptographic technology like that of the Bitcoin blockchain. As a result, the quantum computing threat pertains not only to Bitcoin but also to global financial infrastructure, including payment systems and digital communications.

Concerns about the way that the Bitcoin network will adapt to the quantum threat reflect not only its conservative governance but also the decentralization vector slowing its rate of change. Resistance to rapid change is both a constraint and a safeguard against bad code that causes systemic vulnerabilities.

The structural impediments to Bitcoin not only present challenges to upgrading the network in response to threats but also complicate changes to its monetary policy. If Bitcoin becomes resistant to change in response to hypothetical quantum challenges, altering its 21-million supply schedule will be even more difficult. From that perspective, Bitcoin's caution represents a tradeoff between adaptability and assurance, which will continue to shape its long-term evolution.

Endnotes

1. Figures based on data from Project Eleven and Glassnode as of February 17, 2026. P2PK (Pay-to-Public-Key) is a legacy Bitcoin address type where funds are locked directly to a full public key. It was widely used in the early history of Bitcoin. P2TR (Pay-to-Taproot) is a modern Bitcoin address type introduced with Taproot that locks funds to a Schnorr public key and enables more private and efficient spending conditions. These two address types are known to be vulnerable to quantum computers.

2. Nakamoto, S. 2010. “Bitcoin Talk. Re: Major Meltdown.” Satoshi Nakamoto Institute.

3. Lindell, Y. 2026. “Coinbase Establishes Independent Advisory Board on Quantum Computing and Blockchain.”

4. Swayne, M. 2026. “Ethereum Foundation Elevates Post-Quantum Security To Top Strategic Priority.” Quantum Insider.

5. Zimmerman, M. 2026. “Michael Saylor Says Strategy ($MSTR) Will Lead Global Bitcoin Effort Against Quantum Threats.” Bitcoin Magazine.

6. Jonasnick. “SHRINCS: 324-byte stateful post-quantum signatures with static backups.” Delving Bitcoin. See also Bitcoin Stack Exchange. 2023. “Post-quantum preimage resistance of HASH160 addresses.”

7. Project Eleven. 2026. “Total BTC at Risk of Quantum Attack.”

8. ARK Investment Management LLC. 2026. “Big Ideas 2026. Section 1, The Great Acceleration.”

9. The Cypherpunks/Held, D. 2018. “Planting Bitcoin — Soil (3/4).” Medium.

10. Bluvstein, D. et al. 2023. “Logical quantum processor based on reconfigurable atom arrays. See also Paetznick, A. et al. 2024. “Demonstration of logical qubits and repeated error correction with better-than-physical error rates.” See also Reichardt, B.W. et al. 2024 “Demonstration of quantum computation and error correction with a tesseract code.” Quantum Physics. arXiv. See also Reichardt, B.W. et al. 2024. “Fault-tolerant quantum computation with a neutral atom processor.” Quantum Physics. arXiv. See also Bluvstein, D. 2025. “Architectural mechanisms of a universal fault-tolerant quantum computer.” Quantum Physics. arXiv. See also Kim, Y. 2023. “Evidence for the utility of quantum computing before fault tolerance.” Nature. See also Quantum News. 2025. “IBM Quantum Achieves Milestone: 5,000-Gate Quantum Circuits Unlocked.” Quantum Zeitgeist. See also IBM. 2025. “Scaling for Quantum Advantage and Beyond.” See also Google Quantum AI and Collaborators. 2024. “Quantum error correction below the surface code threshold.” Nature. See also River Lane. 2025. “Quantum Error Correction: Our 2025 trends and 2026 predictions.”

11. Quantum Insider. 2026. “Quantum Computing Companies in 2026: Mapping the Global Quantum Landscape.” See also Wikipedia. N/D. “List of companies involved in quantum computing, communication or sensing.”

12. Tomoshige, H. and P. Singerman. 2026. “Understanding China’s Quest for Quantum Advancement.” Center for Strategic and International Studies. See also See also Boerkamp, M. 2024. “Baidu and Alibaba plan to quit quantum computing research.” Physics World. See also Quantum Strategist.

2024. “Baidu Quantum Donates Quantum Computing Lab to BAQIS, Echoing Alibaba’s Move in Extraordinary Move for China Tech.” Quantum Zeitgeist.

13. Monroe, C. et al. 1995. “Demonstration of a Fundamental Quantum Logic Gate.” Physical Review Letters.

14. Chuang, I.L. et al. 1998. “Experimental realization of a quantum algorithm.” Quantum Physics. arXiv. See also Jones, J.A. et al. 1998. “Implementation of a quantum search algorithm on a quantum computer.” Nature.

15. Cory, D.G. et al. 1998. “Experimental Quantum Error Correction.” Quantum Physics. arXiv.

16. Vandersypen, L.M.K. et al. 2001. “Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance.” Nature.

17. Erixon, F. et al. 2025. “Benchmarking Quantum Technology Performance: Governments, Industry, Academia and their Role in Shaping our Technological Future.” European Centre for International Political Economy. See also Soller, H. et al. 2025. “The Year of Quantum: From concept to reality in 2025.” McKinsey & Company.

18. Alexeev, Y. et al. 2025. “A Perspective on Quantum Computing Applications in Quantum Chemistry using 25--100 Logical Qubits.” Quantum Physics. arXiv. See also Kuhn, M. et al. 2019. “Accuracy and Resource Estimations for Quantum Chemistry on a Near-term Quantum Computer.” Quantum Physics. arXiv.

19. DARPA. N/D. “QB: Quantum Benchmarking.“ See also Altepeter, J. 2024. “Quantum Benchmarking Initiative (QBI).” DARPA. See also Bobier, F-J. et al. 2021. “What Happens When ‘If’ Turns to ‘When’ in Quantum Computing?” McKinsey & company. See also Alexeev, Y. et al. 2025. “A Perspective on Quantum Computing Applications in Quantum Chemistry using 25--100 Logical Qubits.” Quantum Physics. arXiv.

20. Bobier, J-F. et al. 2021. “What Happens When ‘If’ Turns to ‘When’ in Quantum Computing?” Boston consulting Group.

21. National Institute of Standards and Technology. 2026. “Cryptographic Standards and Guidelines

22. Based on data from Glassnode as of February 17, 2026.

23. Unchained Knowledge Base. N/D. “How can I protect my bitcoin against quantum computing?”

24. Check, J. 2025. “One Day, Satoshi's Coins Will Move.” Checkonchain Newsletter. See also River Learn. N/D. “Will Quantum Computing Break Bitcoin?”

25. Roetteler, M. 2017. “Quantum resource estimates for computing elliptic curve discrete logarithms.” Quantum Physics. arXiv.

26. Roettler, M. et al. 2017. “Quantum resource estimates for computing elliptic curve discrete logarithms.” Quantum Physics. arXiv. See also Litinski, D. 2023. “How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates.” Quantum Physics. arXiv.

27. Heilman, E. 2018. “Pay-to-Merkle-Root (P2MR).”cyryptoquick/bips.

28. Ivezic, M. 2025. “Q-Day Revisited – RSA-2048 Broken by 2030: Detailed Analysis.” Postquantum. See also Aarsonson, S. “Quantum computing: too much to handle!” Shtetle-Optimized.

29. Mattdf. 2025. “Why Quantum Computing will take another 50 years.”

30. National Institute of Standards and Technology.. 2025. “Transition to Post-Quantum Cryptography Standards.” See also National Institute of Standards and Technology. 2026. “Frequently Asked Questions about Post-Quantum Cryptography.” See also Mosca, M. and M. Piani. 2024. “Quantum Threat Timeline Report 2024.” Global Risk Institute. See also IBM Technology Atlas.2026. “The future of computing is quantum-centric.2033+.”

31. Gutman, P. and S. Neuhaus. 2025. “Replication of Quantum Factorisation Records with an 8-bit Home Computer, an Abacus, and a Dog.” Cryptology ePrint Archive.

32. Nordhaus, W.D. 2007. “Two Centuries of Productivity Growth in Computing.” The Journal of Economic History. See also Koomey, J. et al. 2011. “Implications of Historical Trends in the Electrical Efficiency of Computing.” IEEE Annals of the History of Computing.

33. Aaronson, S. 2009. “Hopefully my last D-Wave post ever.” Shtetle-Optimized.

34. Parker, E. and M.J.D. Vermeer. 2023. “Estimating the Energy Requirements to Operate a Cryptanalytically Relevant Quantum Computer.” Rand.

35. Gidney, C. and M. Ekerå. 2021. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.” arXiv.

36. National Institute of Standards and Technology. 2024. “NIST Releases First 3 Finalized Post-Quantum Encryption Standards.”

37. National Institute of Standards and Technology. 2024. “Module-Lattice-Based Digital Signature Standard.” Computer Security Research Center.

38. National Institute of Standards and Technology. 2024. “FIPS 205 Stateless Hash-Based Digital Signature Standard.” Computer Security Research Center.

39. Open SSH. N/D. “Post-Quantum Cryptography.” See also Help Net Security. 2025. “OpenSSL prepares for a quantum future with 3.5.0 release.”

40. BIP 360. 2025. “BIP 360 to enable Pay-to-Merkle-Root: a proposed first step in advancing Bitcoin quantum resistance.”

41. Kudinov, M. and J. Check. 2025. “Hash-based Signature Schemes for Bitcoin.” Cryptology ePrint Archive.

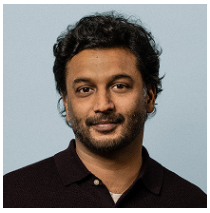
42. Kudinov, M.2025. “Hash-Based Signatures for Bitcoin's Post-Quantum Future.” Bitcoin Development Mailing List.
See also Jonasnick. 2025. “SHRINCS: 324-byte stateful post-quantum signatures with static backups.” Delving Bitcoin.

43. Cypherpunk Cogitations. 2025. “Against Allowing Quantum Recovery of Bitcoin.”

44. Check, J. 2025. “One Day, Satoshi's Coins Will Move.” Checkonchain Newsletter.

45. Crypto 101. 2023. “What was the Blocksize War?” Bitstamp Learn.

About The Authors



Dhruv Bansal

Co-Founder and CSO
at Unchained

@dhruvbansal

Dhruv co-founded Unchained in 2016. As Chief Science Officer, he focuses on bitcoin infrastructure, distributed systems, and research into collaborative custody and financial services built around multisignature security.

Prior to Unchained, he co-founded the data-science startup Infochimps in 2008, which was later acquired by CSC in 2013. He previously studied mathematics and physics at Columbia University and pursued doctoral research in statistical physics at the University of Texas at Austin, where his work on complex networks led him toward large-scale data analysis and distributed computing. Dhruv writes and speaks frequently about bitcoin and decentralized systems, including research such as the HODL Waves and HODL Cave metrics and the “Bitcoin Astronomy” series exploring the long-term implications of bitcoin networks and markets.

Tom Honzik

Director of Custody Research
at Unchained

@tom_honzik

Tom joined Unchained to help individuals and businesses understand how to securely hold their own bitcoin. As Director of Custody Education, he focuses on long-term bitcoin custody, multisignature security, and practical guidance for successfully managing private keys and UTXOs.

Through client onboarding, research, and educational writing, he has helped thousands of individuals and organizations learn how to better secure their own bitcoin treasuries using collaborative multisignature wallets. He regularly publishes technical explainers on bitcoin wallet architecture, address types, and custody tradeoffs, and has built a library of contributions ranging from basic introductory material to advanced structural analysis.

David Puell

Research Trading Analyst/
Associate Portfolio Manager,
Digital Assets at ARK Invest

@dpuellARK

David joined ARK Invest in January 2022. As Research Trading Analyst and Associate Portfolio Manager for Digital Assets, he focuses on Bitcoin and cryptoasset on-chain and market research.

Prior to ARK, he was Head of Research at Adaptive Capital in 2019 and 2020. He is best known for pioneering the emergent field of cryptocurrency on-chain analysis and has created a dozen metrics used industry-wide today, including the MVRV Ratio and the Puell Multiple. His metrics are featured in most major cryptoasset data platforms such as Glassnode, Coin Metrics, and CryptoQuant. David has been quoted in Bitcoin Magazine, Coindesk, among other publications, and has been featured in the Bitcoin Magazine Podcast, Will Clemente’s Blockware Intelligence Podcast, and The Pomp Podcast.

DISCLOSURE

The paper reflects the collaboration of Dhruv Bansal, Tom Honzik, and David Puell. Dhruv Bansal is Co-Founder and CSO at Unchained. Tom Honzik is Director of Custody Research at Unchained. David Puell is Research Trading Analyst and Associate Portfolio Manager for Digital Assets at ARK Investment Management LLC ("ARK"). Unchained is a private, bitcoin-native financial services company, and is unaffiliated with ARK. The views and opinions expressed herein are those of the individual authors and are provided for informational and educational purposes only, and do not necessarily reflect the official positions or views of either Unchained or ARK (collectively, "The Firms"). The Firms disclaim any liability for any loss arising from reliance on this material.

Certain of the statements contained in this presentation may be statements of future expectations and other forward-looking statements that are based on ARK's current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. The matters discussed in this presentation may also involve risks and uncertainties described from time to time in ARK's filings with the U.S. Securities and Exchange Commission. ARK assumes no obligation to update any forward-looking information contained in this presentation.

ARK and its clients as well as its related persons may (but do not necessarily) have financial interests in securities or issuers that are discussed. Certain information was obtained from sources that ARK believes to be reliable; however, ARK does not guarantee the accuracy or completeness of any information obtained from any third party.

ARK Invest Management LLC
St. Petersburg, FL 33701

info@ark-invest.com
www.ark-invest.com

Unchained
Austin, TX 78767

hello@unchained.com
www.unchained.com

Join the conversation on X
@ARKinvest @unchained