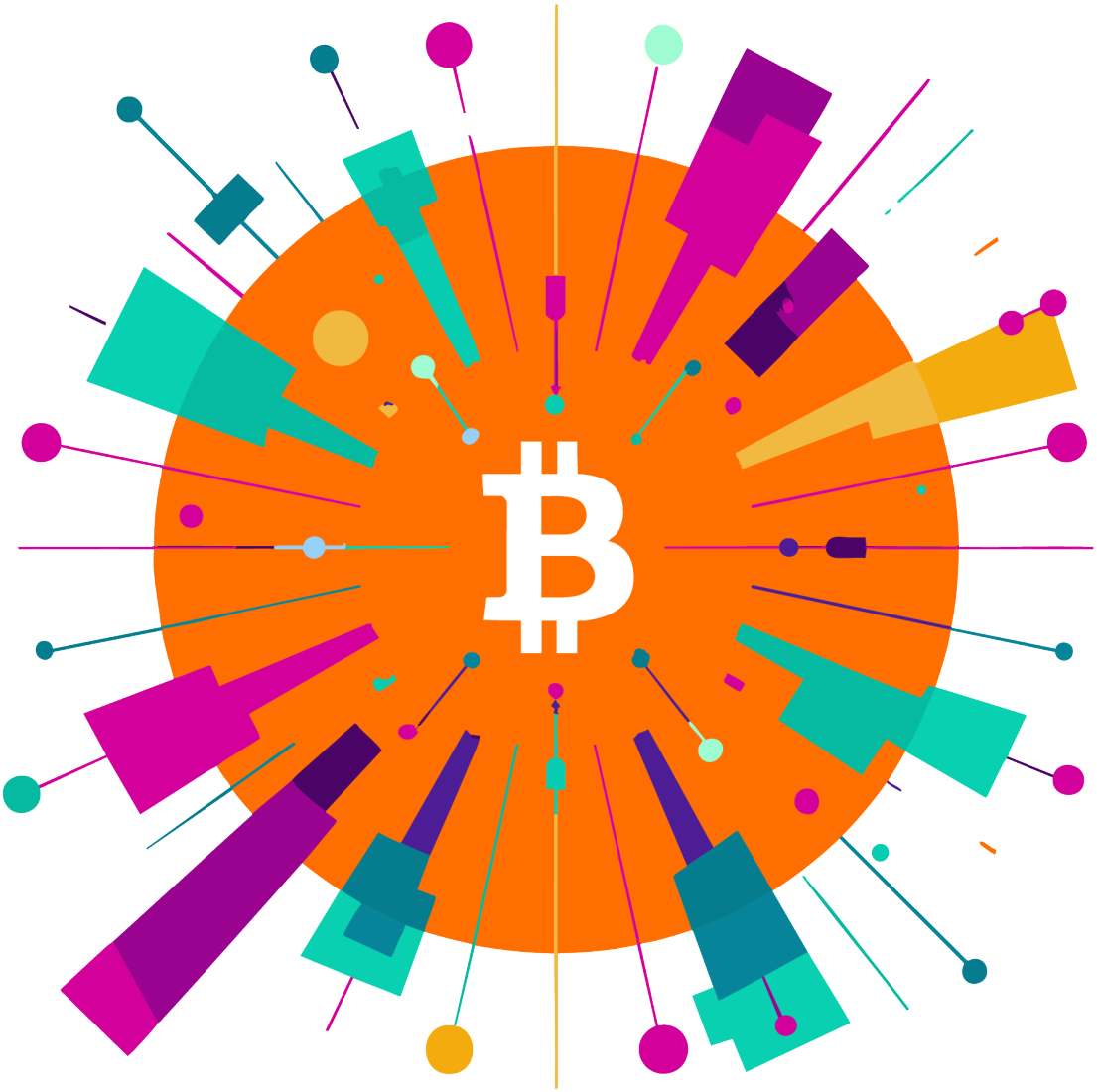
chaincode

May 2025

Bitcoin and Quantum Computing:
Current Status and Future Directions



Dr. Anthony Milton
Dr. Clara Shikhelman

The authors would like to thank Ethan Heilman, Gloria Zhao, Shai (Deshe) Wyborski, Alan Szepieniec and Stephen DeLorme for their time and efforts in review.

Table of Contents

1. Executive Summary

- **Cryptographically relevant quantum computers (CRQCs) pose a significant threat to Bitcoin**, potentially enabling the theft of ~6.26 million BTC (~US$650 billion) and destabilizing the entire ecosystem. Funds most vulnerable to CRQCs are large institutional and exchange holdings, where public keys have been exposed due to "address reuse" practices, and Satoshi-era funds due to script type.

- **Quantum computing's potential impact on Bitcoin mining appears limited by its lack of effective parallelism, along with inherent algorithmic, economic, and hardware constraints, unlike its clear threat to Bitcoin's cryptography.** Still, there is the potential for network instability due to correlated fork events if aggressive quantum mining strategies are pursued, and there is a centralization risk if quantum mining becomes dominant.

- **Preparing Bitcoin for the quantum era will demand community-wide decisions rooted in philosophical and ideological questions**, including the question of whether quantum-vulnerable funds should be "burnt" or if they should be available for "stealing" by those with access to CRQCs. Broader engagement is important and still largely lacking.

- **Several leading cryptographers and Bitcoin developers - such as Tim Ruffing, Jonas Nick, and Ethan Heilman - are actively working on Bitcoin's quantum readiness, joined by a number of new and enthusiastic contributors.** Current strategies include quantum-resistant signature approaches such as Lamport signatures, quantum-secure Taproot scripts, and pay-to-quantum-resistant-hash, and migration approaches such as commit-delay-reveal. Discussions about these efforts are ongoing across GitHub, the Bitcoin Development Mailing List, the Delving Bitcoin forum, and other public channels. However, all of these initiatives, including those with publicly visible components, remain at an early and exploratory stage, with much of the preliminary research still occurring informally and privately.

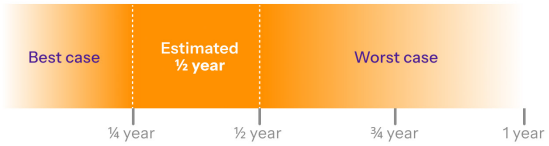
- Expert and governmental estimates regarding the pace of quantum computing development suggest CRQCs could arrive within the next decade. **We propose a dual-track strategy for action that balances urgent security needs with thorough research: rapidly developing contingency measures (within approximately 2 years) that can be quickly deployed if needed while simultaneously pursuing a comprehensive ~7 year path to optimal quantum resistance.** This approach positions Bitcoin to respond flexibly and securely to a range of possible quantum scenarios, including a rapid escalation in quantum computing capabilities.

Upgrade Timeline

Here are estimated timelines for short-term contingency measures as well as a long-term comprehensive solution. With this dual track strategy, each track can be worked on in parallel.

Short-term Contingency Measures (~2 Years)

Phase 1: Research + BIP



Phase 2: Implementation

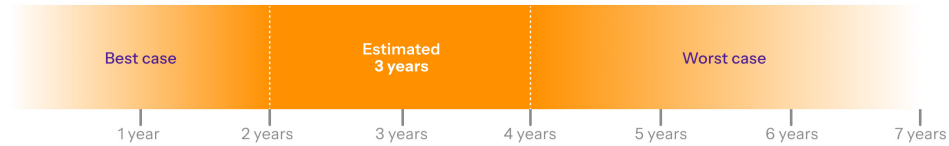
Phase 3: Migration

Long-Term Comprehensive Path (~7 Years)

Phase 1: Research + BIP

Phase 2: Implementation

Phase 3: Migration



2. Introduction

Bitcoin relies on a cryptographic assumption long regarded as computationally infeasible to break with current technology and approaches. However, the arrival of Cryptographically Relevant Quantum Computers (CRQC), potentially within the next decade, threatens to undermine this assumption. This report examines the nature of this threat, investigates the technical proposals and governance challenges that Bitcoin must address, and proposes approaches and timelines to ensure Bitcoin's security against quantum computing threats, whenever they may arise.

A key component of Bitcoin's cryptographic foundation is Elliptic Curve Digital Signature Algorithm (ECDSA) and, since 2021, Schnorr signatures. Both rely on the computational difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), which presents an asymmetric challenge: deriving a public key from a private key is computationally simple, while the reverse operation would take current supercomputers trillions of years. This asymmetry collapses when faced with CRQCs, potentially reducing the time to derive a private key from a public key to mere hours or days.

While no quantum computer today poses an immediate risk to Bitcoin, a third of the respondents in a recent survey of global experts indicated a likelihood of 50% or more that CRQCs capable of breaking Bitcoin's cryptography could emerge between 2030-2035. This aligns with directives from the National Institute of Science and Technology (NIST), the wider U.S. Government, and other governments and institutions from around the world to deprecate vulnerable cryptographic standards like Elliptic Curve Cryptography by 2030 and disallow them by 2035.

The potential impact to Bitcoin were a CRQC to appear is substantial. Analysis suggests that approximately 20-50% of all Bitcoin in circulation (4-10 million BTC), worth hundreds of billions of dollars, is vulnerable to being stolen by virtue of private keys being derived from public keys. This includes outputs controlled by exposed public keys, either through the use of certain vulnerable script types or through "address reuse" after spending. The most susceptible funds are certain exchange and institutional addresses (due to address reuse) and Satoshi-era holdings and presumed lost coins (due to vulnerable script types); those that hold substantial value, such as the exchange and institutional addresses, are especially attractive targets for quantum-enabled theft.

In addition, quantum computing could also impact Bitcoin mining. However, this scenario is significantly less likely in the foreseeable future. Mining performance is primarily determined by clock speed, and quantum miners would need to compete with highly optimized ASICs. Despite the quadratic speed-up potential of quantum miners, such an advantage remains insufficient to outperform classical miners without dramatic improvements in quantum computing capabilities, something that is not expected anytime soon.

If this were to transpire, it could open the door to double-spend attacks by small or medium-scale miners, and a shift toward dominant quantum mining could introduce new risks of mining centralization. While such scenarios are likely far off, exploring post-quantum mining remains a topic of theoretical interest and may help inform future preparedness.

Beyond these direct threats of broken cryptography and mining turbulence, there are broader ecosystem components, from SSL/TLS to hardware wallets, that could be compromised in a post-quantum environment, compounding the security challenges faced by Bitcoin stakeholders.

The content that follows is an exposition of the various facets of the quantum computing threat to Bitcoin, beginning with the state of quantum computing in 2025. Following this is a comprehensive examination of exactly how Bitcoin is at risk: public key exposure in certain script types enabling long-range attacks, short-range vulnerabilities during transaction broadcasts or shortly after confirmation, potential mining centralization with quantum mining, and ecosystem vulnerabilities.

The post-quantum efforts in Bitcoin are then examined, including the general concepts and technical proposals that are currently under consideration. Central to the discussion is a fundamental dilemma facing the Bitcoin community: whether to "burn" vulnerable coins or leave them susceptible to being "stolen" by entities with CRQCs. Following this is an evaluation of the potential migration pathways for moving quantum-vulnerable funds to quantum-resistant scripts. Finally, the report outlines 2 timelines for action, one representing a short-term contingency measure and the other a longer-term comprehensive path on par with similarly significant changes to Bitcoin (SegWit and Taproot), before concluding with the key considerations of Bitcoin's post-quantum transition.

This report provides a systematic analysis of the quantum threat landscape and evaluates the technical, economic, and governance challenges that Bitcoin faces in this transition. By examining both the technical proposals under consideration and the complex social coordination required to implement them, this report aims to accelerate the consensus-building process that must begin now, years before CRQCs can break Bitcoin's cryptographic foundations. The stakes extend beyond the hundreds of billions of dollars in vulnerable Bitcoin - this may be the most significant test of Bitcoin's decentralized governance model to date, requiring the community to balance security imperatives with core principles of property rights, censorship resistance, and conservatism. The window for careful, deliberate action exists today, but will narrow as quantum computing advances, making proactive preparation not merely prudent, but essential for Bitcoin's long-term survival.

3. Quantum Computing

Quantum computing offers a potentially transformative approach to computation by leveraging the principles of quantum mechanics. This enables quantum computers to achieve significant speed-ups in solving specific classes of problems that are intractable for classical systems.

While quantum computing has the potential for transformative applications in many areas, including cryptographic techniques integral to Bitcoin, significant challenges remain before this potential is realized. Quantum systems are highly sensitive to environmental disturbances, making them prone to errors, and building practical, large-scale quantum computers requires overcoming substantial technical hurdles in both hardware stability and error correction.

Although the last few years have seen significant progress as major technology companies and research institutions make breakthrough advancements in the field, quantum computers are still nascent and have not yet achieved the stability, capability, and scale to be useful in any commercially relevant application. Despite this, a recent 2024 survey of 32 global experts from academia and industry, revealed that almost a third of the respondents (10/32) indicated a likelihood of about 50% or more of Cryptographically Relevant Quantum Computers (CRQC), quantum computers that are powerful enough to break widely used cryptographic systems in a reasonable period of time, appearing in the next 10 years [MP24].

State of Quantum Computing in 2025

The quantum computing landscape in early 2025 is characterised by recent significant announcements from major industry players such as Google and Microsoft. Google's "Willow" quantum processor, announced in December 2024, achieved a crucial milestone in quantum error correction[1] [Nev24]. And while the 105 physical qubit Willow processor's performance on the Random Circuit Sampling (RCS) benchmark is undeniably impressive, its significance remains confined to that specific task and does not extend to broader applications.

In February 2025, Microsoft unveiled "Majorana 1" which it claimed was the world's first quantum processor powered by Majorana particles and topological qubits [Nay25]. Their new approach to building a quantum processor purportedly provides a clear path to scaling to a million qubits on a single chip, with topological qubits being intrinsically resistant to local environmental disturbances. However, the scientific community has expressed some skepticism regarding Microsoft's claims, particularly about whether the observed phenomena truly represent topological qubits [Bal25, Rin25].

Other key players in the industry have also made strides recently: IBM Quantum announced its IBM Quantum System Two, featuring 133 physical qubit IBM Quantum Heron processors

1 They demonstrated "below threshold" performance whereby adding more physical qubits for error correction actually improved performance rather than increasing the error rate. Below threshold has been an outstanding engineering challenge in quantum error correction.

(December 2023) [Gam24]; Amazon Web Services announced its first in-house quantum chip "Ocelot" in February 2025 [BP25]; and Quantinuum launched a 56 physical qubit trapped-ion quantum computer in June 2024 [Qua24].

Despite these advancements, the timeline for, or even just the viability of, commercially relevant quantum computers remains a divisive topic. If a general-purpose, commercially relevant quantum computer can indeed be built, it is widely acknowledged to require on the order of ~1000 logical qubits[2] at a minimum. IBM Quantum's development and innovation roadmap projects them reaching ~1000's of logical qubits from the year 2033 onwards [IBM24] while Intel announced in February 2025 a partnership with Japan's AIST to realize a system with tens of thousands of logical qubits at an industrially usable level by the early 2030s [AIS25].

In September 2024, Scott Aaronson, a leading expert in quantum computing theory, and famously a pessimist on the time horizon for CRQCs and the threat to current cryptosystems, proclaimed: "*I think today that message needs to change. I think today the message needs to be: yes, unequivocally, worry about this now. Have a plan (for migrating from RSA and Diffie-Hellman and elliptic curve crypto to lattice-based crypto, or other systems that could plausibly withstand quantum attack)*" [Aar24]. Hartmut Neven, head of Google Quantum AI, believes commercial applications in areas like materials science, medicine, and energy could be seen within the next five years, whereas NVIDIA's Jensen Huang believes practical uses for quantum computers are still about 20 years away [Che25]. Again, it's important to recognize that, to date, no quantum computer has outperformed a supercomputer on any commercially relevant application[3]; superior performance has only been achieved on benchmarks such as RCS.

2 The ratio of underlying physical qubits to logical qubits is on the order of 10x to 1000x, varying with the methodologies and technologies used to physically realize qubits, correct errors etc.

3 A paper published in Nature in March 2025 outlined an experimental demonstration of an RCS-based certified randomness protocol, which could have commercial relevance [LSN+25].

4. Threat Model: Quantum Risk to Bitcoin

Bitcoin's security relies on cryptographic primitives designed to be computationally infeasible to break with classical computing algorithms and hardware. The potential emergence of CRQCs threatens to fundamentally break this cryptographic foundation. This section provides a systematic analysis of quantum computing threats to Bitcoin, examining the susceptibility of public key cryptography to quantum attacks, the varying exposure levels of different Bitcoin script types, and additional factors that place funds at risk. The potential weaknesses of cryptographic hash functions when faced with quantum algorithms are outlined, and the implications for Bitcoin mining and network security are examined.

Public Key Vulnerability and Bitcoin Theft

Elliptic Curve Cryptography (ECC) is a key cryptographic technology used in Bitcoin for digital signatures. Bitcoin originally only used the Elliptic Curve Digital Signature Algorithm (ECDSA) but with the Taproot upgrade in 2021, Bitcoin also began supporting Schnorr signatures (both use the secp256k1 curve). Schnorr signatures offer several advantages over ECDSA, including simpler design, stronger security properties, and support for key aggregation in multi-signature setups [Shi21].

Despite their differences, both ECDSA and Schnorr signatures rely on the same underlying computational security assumption: the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP) over the secp256k1 curve. At the heart of ECDLP is an asymmetry in computation using classical computing techniques:

- It's relatively fast to compute the forward operation, that is, derive a public key from a private key. This takes on the order of microseconds on a personal computer [PHN+24].
- The reverse operation, deriving a private key from a public key for Bitcoin's current signature schemes, is computationally infeasible with classical computers, requiring ~2^{128} operations [Nak18], which would take the current top supercomputer of November 2024 more than 100 quadrillion (10^{17}) years to compute for a single private-public key pair[4].

This asymmetry collapses with the advent of quantum computers capable of running **Shor's algorithm**. Shor's algorithm is a quantum algorithm that efficiently solves the discrete logarithm problem, requiring many orders of magnitude fewer operations than classical approaches. A CRQC running Shor's algorithm could potentially derive a private key from a public key in a matter of hours to days [Lit23], effectively breaking both ECDSA and Schnorr signature schemes. In fact, all public key cryptography schemes that rely on the asymmetry of ECDLP or a similar asymmetry of large integer factorization (such as RSA) are broken in the face of CRQC. The capability of CRQCs to derive a private key from a public key represents

4 The 100 quadrillion years figure is based on the El Capitan system having ~11.04 million CPU cores running at 1.8GHz capable of ~1.99×10^{16} cycles/second, ~2^{128} elliptic curve group operations (Pollard's rho algorithm), 3000 cycles/elliptic curve operation etc [SDS+24].

the most significant quantum threat to Bitcoin, as an attacker can use a quantum-derived private key to steal Bitcoin by creating and broadcasting a valid transaction that spends the victim's UTXOs to an address they control.

This capability manifests in two distinct attack vectors, long-range attacks and short-range attacks. **Long-range attacks** target funds associated with public keys already exposed on the blockchain, making these funds perpetually vulnerable until moved to address types that don't reveal public keys on-chain. **Short-range attacks** (also known as front-running attacks or transaction hijacking attacks [SIZ+18]) operate within the limited timeframe when transactions reveal previously concealed public keys during spending, requiring attackers to derive the private key within a narrow window of time. These attack vectors create a spectrum of quantum vulnerability in Bitcoin's UTXO set, with vulnerability determined by script type and public key exposure.

Vulnerability Classification by Bitcoin Script Type

The existence of CRQCs is one matter, the other consideration for private key derivation is actually having access to public keys so that the corresponding private keys can be derived. This requirement impacts the set of spendable Bitcoin, the Unspent Transaction Outputs (UTXOs), in an uneven fashion, and there are different risks depending on script (output) type and use (e.g., if an address has been re-used). The following describes the various script types and their level of vulnerability.

Immediately Vulnerable Script Types

Three of Bitcoin's script types are immediately vulnerable to CRQCs: P2PK (Pay to Public Key), P2MS (Pay to MultiSig), and P2TR (Pay to TapRoot). These scripts are vulnerable because they expose a public key or public keys when they are used as the destination in a transaction. More specifically, elliptic curve public keys that are vulnerable to quantum private key derivation are present in the locking script (ScriptPubKey) for all to see without any obfuscation. The Bitcoin blockchain is thus a public record of such public keys; any corresponding UTXOs are vulnerable via long-range attack until they are successfully spent (to less susceptible script types).

Legacy Bitcoin output types P2PK and P2MS both present ECDSA public keys directly in their locking scripts, making them vulnerable to quantum attacks. P2PK, one of Bitcoin's original output types used for early mining rewards [BSE18], represents only ~0.025% of current UTXOs but locks a disproportionate ~8.68% of Bitcoin's value (~1,720,747 BTC) [Erh23]. This is overwhelmingly in dormant Satoshi-era coins - in the past 2.5 years there have been ~67 new P2PK UTXOs created. Similarly vulnerable is P2MS, the "raw multisig" format introduced in 2011 that has since been replaced by more advanced multisig implementations [And11]. While P2MS accounts for ~1.037% of UTXOs, these secure a mere ~57 BTC [Erh23].

Pay to Taproot (P2TR), introduced in the 2021 Taproot soft fork [WNT20], exposes public keys in a different but equally vulnerable manner. P2TR provides two spending mechanisms: the key-path and the script-path. The key-path allows spending using a signature from a "tweaked key" (a public key combined with a commitment hash of possible script conditions), while the script-path requires revealing and satisfying one of these predefined script conditions.

Because the tweaked public key is exposed on the blockchain, a CRQC could potentially derive the corresponding private key, enabling unauthorized spending via the key-path without needing to satisfy any script conditions. Unlike P2PK and P2MS, P2TR's vulnerability could be addressed through a soft fork that disables key-path spending if quantum threats emerge (see Lamport Signatures with OP_CAT, Quantum-Secure Taproot Scripts). Currently, P2TR outputs constitute ~32.5% of all UTXOs but represent only ~0.74% of Bitcoin's total value (~146,715 BTC) [Erh23].

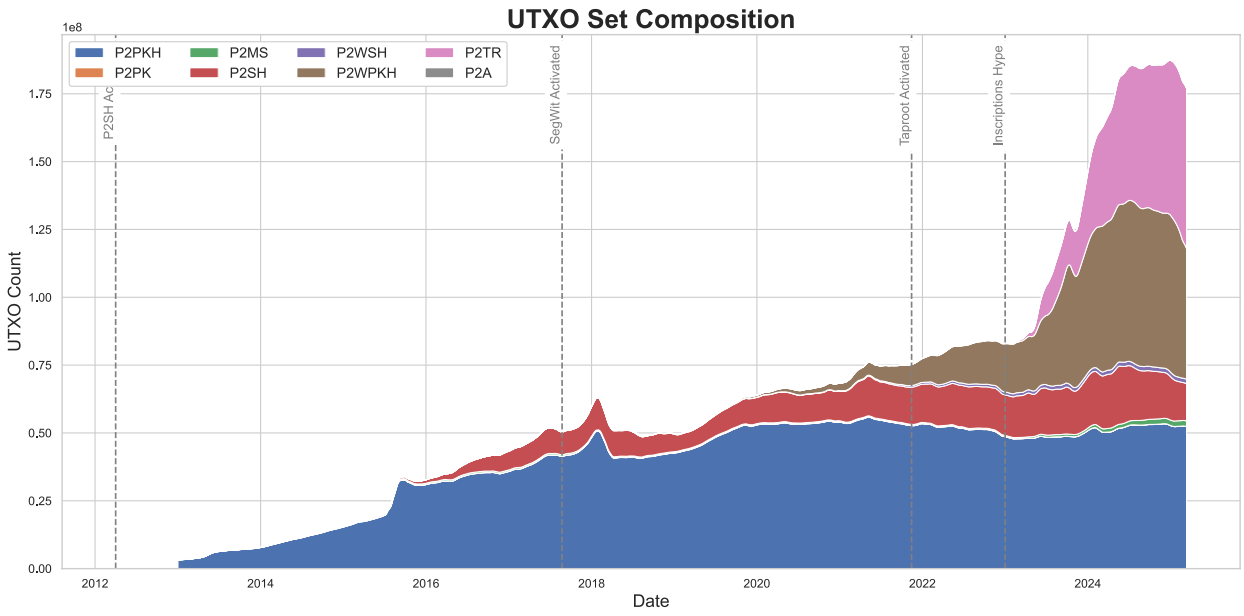


Figure 1. UTXO set size and composition by script type, adapted from [MO25d].

On-Spend Vulnerable Script Types

P2PK, P2MS and P2TR are all vulnerable from the moment they receive funds, as they expose public keys directly in the output script. This makes them vulnerable to long-range attacks - public keys are visible over a potentially long period of time for an attacker to exploit. The other script types in Bitcoin, however, are not vulnerable in the same way (as soon as coins move to them), but are instead vulnerable to a CRQC deriving private keys when they reveal the public key at the moment they are spent from.

All of Bitcoin's current script types share this spending-time, momentary vulnerability. When spending from any script type, public key(s) are exposed as part of the unlocking script. When the transaction is in mempools across the network, these public keys(s) are open for all to see, so an attacker with a CRQC could potentially derive the corresponding private key(s) and then sign and broadcast a competing replacement transaction, or could directly mine it without broadcasting. This could be either before the original transaction confirms, or the attacker could either attempt themselves, or incentivize others, to do a chain reorg. If this is the first and only time the public key(s) are revealed, the vulnerability window is limited to the period when the transaction remains unconfirmed in mempools or has been mined in a recent block, hence the term short-range attack.

Address Reuse Vulnerability

If the public keys of one of the less susceptible script types (P2PKH, P2SH, P2WPKH, P2WSH) have already been exposed, such as through a previous spend from the same address, then these scripts also become vulnerable to long-range attacks. This is because once a public key has been revealed on the blockchain, it remains visible forever, giving an attacker time to derive the private key. Although address re-use is recognized to be bad for privacy, it remains a common practice. It is also particularly dangerous in a post-quantum environment as it transforms script types that would normally only be vulnerable to short-range attacks into ones that are vulnerable to long-range attacks.

Other Avenues for Public Key Exposure

Although not strictly address re-use, public keys will have been exposed for a UTXO on Bitcoin if the corresponding UTXO was spent on a fork like Bitcoin Cash or Bitcoin Gold. When Bitcoin was forked in 2017, the UTXO set was duplicated across chains, meaning users owned identical outputs on both networks. When spending these outputs on fork chains, users revealed the public keys associated with their Bitcoin UTXOs, even if they haven't yet spent those UTXOs on the Bitcoin network. With significant Bitcoin fork activity during 2017-2019, this exposure affects a potentially non-trivial portion of Bitcoin's UTXO set.

There are also many UTXOs whose public keys are known to multiple parties but not to the entire world. Extended public keys (xpubs) allow for generation of public keys (addresses) without the need to know the corresponding private keys - they have effectively become the standard means for service providers to track payments on behalf of the user without having spending authority. They are commonly used throughout the Bitcoin ecosystem, with many services, including exchanges, wallet providers, payment processors, and custody solutions, requiring customers to provide xpubs to enable functionality like generating new receive addresses and monitoring for transactions without user input.

With an xpub being a public key, they are vulnerable to the corresponding private key being derived by a CRQC. And while the risk varies depending on hardening practices, derivation paths, and the security of xpub sharing, it's crucial to recognize that CRQCs fundamentally change the xpub security model. A quantum computer with access to an xpub and its chain code could derive, through simple iteration, all non-hardened child public keys, and thus all corresponding private keys. This creates a cascading vulnerability where a single exposed xpub could compromise all funds held in non-hardened derivation paths (hardened child keys remain secure).

It's worth noting that for users who use xpubs to derive addresses to transact with, but otherwise keep their xpubs private, CRQCs don't introduce new linkability concerns. That is, CRQCs can't be used to reveal links between addresses derived from the same (private) xpub, and currently unlinkable transactions will remain unlinkable. This maintains the distinction between the derivation security model (child key → parent key), which utilizes one-way hash functions[5], and the public key cryptography security model (public key → private key), which relies on ECC.

5 Almost all modern wallet software uses Hierarchical Deterministic (HD) key generation which leverages the HMAC-SHA512 algorithm in accordance with BIP-32 [Wui12].

Other examples of public keys known to multiple parties but not publicly include multisignature arrangements, which require multiple participants to know each other's public keys to construct and verify transactions. The Lightning Network necessarily exposes channel public keys to both participants during channel establishment and operation. Similarly, some escrow services and shared custody solutions implement multisignature schemes where multiple parties must have knowledge of other parties' public key material[6]. While the limited exposure reduces the likelihood of a broad attack, it also creates scenarios where insiders with technical capability might face perverse incentives to attempt targeted quantum attacks once the technology becomes available.

Ecosystem Vulnerabilities

If ECC is broken by CRQC, the implications extend far beyond Bitcoin - most internet cryptosystems would be vulnerable, assuming they have not yet been upgraded for post-quantum. Core protocols like SSL/TLS may no longer be secure (though work on this front is well underway, see Post-Quantum Cryptography in Industry). Bitcoin may then be susceptible to "ecosystem" attacks like Man-in-the-Middle (MITM) attacks, where an attacker could subvert SSL to intercept connections with exchanges and maliciously redirect users [Hoy18]. Other similar ecosystem vulnerabilities might include compromising hardware wallet firmware updates, infiltrating mining pools by spoofing authentication, attacking DNS to redirect users to malicious nodes or exchanges, or compromising blockchain API services that many applications rely on. These vectors are particularly dangerous because they leverage the broader technical infrastructure that Bitcoin depends on, potentially allowing attackers to remain undetected longer than if they were just performing UTXO theft by CRQC private key derivation.

Bitcoin's Hash Functions and Grover's Algorithm

Cryptographic hash functions are another of Bitcoin's key cryptographic pillars that could be impacted by the arrival of CRQCs. Two hash functions are used in Bitcoin, SHA-256 and RIPEMD-160, with SHA-256 being used for a variety of purposes including mining (hashing of block headers to "mine" a block), generating transaction IDs, signing transactions, checksums and generating public key hashes (in combination with RIPEMD-160 in the form of HASH-160) [Wal25]. In the context of CRQCs, the use of the hash functions that warrant closer examination is the use in mining.

A key property of cryptographic hash functions such as SHA-256 and RIPEMD-160 is that they are irreversible: given some output of the hash function, it's computationally infeasible to establish the original input data. This computational infeasibility can be characterized as requiring a brute-force search through all possible inputs. Finding the input corresponding to some SHA-256 output would take the current top supercomputer of November 2024 many orders of magnitude longer than it would take to derive a Bitcoin private key from a public key[7].

---

6 Others use threshold signature schemes (TSS) which distribute key shares among multiple parties without requiring complete knowledge of others' key material to reconstruct signatures.

7 It might take El Capitan on the order of $1x10^{17}$ years to derive a private key from a public key, but it would take on the order of $1x10^{53}$ years to find a preimage for some SHA-256 output.

Grover's algorithm is a quantum algorithm that affords a speedup over classical approaches to problems such as finding the input corresponding to some hash function output. More formally, Grover's algorithm gives a quadratic speedup for unstructured search problems, reducing the number of required operations to find a solution from O(N) (parallelizable) to O(√N) (sequential) [Gro96]. For Bitcoin, the implication is that the security of SHA-256 and RIPEMD-160 is somewhat weakened, but by no means broken. Even with the quantum advantage of Grover's algorithm, breaking these hash functions would require an exceptionally capable CRQC, one that far exceeds the capabilities of any foreseeable CRQC in the near to medium term (if indeed CRQCs will one day be realized)[8] [ADM+16].

Impact on Bitcoin Mining

Unlike quantum attacks on digital signatures, quantum mining must compete with classical mining. In the case of Bitcoin's ECC-based signatures, once quantum computers reach sufficient scale, a single machine (CRQC) can compromise funds by breaking the underlying cryptography. Quantum mining, by contrast, requires a large fleet of fast quantum machines to match the performance of today's ASICs. Unlike classical mining, quantum mining cannot be easily parallelized[9], making it significantly harder to scale and much less efficient in practice.

Bitcoin mining is the computational process of finding a block header hash that satisfies the Bitcoin network's difficulty requirement. Miners construct a block of transactions, then repeatedly hash the block header (using SHA-256) while varying the nonce value and other fields until they find a hash value that is below the difficulty target. A miner that is successful in finding such a hash value, and has their block recognized as belonging to the longest chain[10] by the network, earns the mining reward - newly minted bitcoins from the block subsidy as well as the fees from transactions they included in the block. There are substantial computational resources participating in mining that are securing the network by competing against each other to add blocks to the blockchain in this manner. This proof-of-work (PoW) process also makes it prohibitively difficult to alter past transactions.

Bitcoin was designed to consistently produce blocks at a rate of approximately one block every 10 minutes. To maintain this target, the network automatically adjusts the difficulty target every 2016 blocks (roughly every two weeks) based on the time taken to mine the previous 2016 blocks. This adjustment is effectively a response to changes in the total computational power dedicated to mining - as more miners join (leave) the network or deploy more efficient hardware, the difficulty increases (decreases) proportionally.

While Grover's algorithm provides a theoretical quadratic speedup for the hash-based PoW in Bitcoin mining, qualifying the risks of quantum mining - the application of quantum computing and Grover's algorithm to Bitcoin mining - has been an area of

8 The ~2^{255} classical operations become ~2^{128} ($3.4*10^{38}$) quantum operations.

9 This arises from a fundamental property of Grover's algorithm and is not just a limitation of technology, see [Dea25].

10 Generally the longest chain is the one representing the most accumulated work.

active research [BGN+22]. Bitcoin mining is a highly dynamic component of Bitcoin; it evolves continuously with increasing hash rates, difficulty target adjustments, specialized hardware (ASIC) development, and varying economic incentives. This dynamic nature means quantum mining's impact depends not only on quantum computing capabilities but also on how the classical mining ecosystem evolves in parallel.

Forks and 51% Attacks

Research indicates that quantum mining could introduce timing challenges that don't align with Bitcoin's 10-minute block discovery rhythm. When another miner finds a block, quantum miners must choose between 'aggressive' strategies (measuring their current state and potentially creating competing blocks) or 'peaceful' approaches (abandoning computation to start fresh) [NG21]. The pursuit of aggressive strategies could substantially increase the rate of stale blocks (valid blocks that are ultimately excluded from the main chain), as many quantum miners measuring their states simultaneously in response to new blocks would create correlated fork events [BS24, Sat18].

A higher frequency of forks has security implications for the Bitcoin network - when forks occur, honest mining power becomes divided across competing chains, whereas an attacker can strategically concentrate their resources on a single chain. This division of honest computational power effectively reduces their collective influence on the longest chain, potentially allowing attackers with less than half of the network's total computational power to execute 51% attacks.

Mining Centralization

Bitcoin's mining ecosystem already demonstrates significant centralization due to the "superlinear problem," where larger miners gain advantages beyond their proportional computing contribution through economies of scale, superior hardware efficiency, and geographic advantages, and also through behaviors such as selfish mining. However, the arrival of quantum computing would fundamentally transform this dynamic into something far more extreme through what researchers term the "quantum superlinearity problem" [PS22].

Quantum computers implementing Grover's algorithm would provide a quadratic speedup that disproportionately benefits the miners with the best quantum hardware[11], creating a scenario where such miners *"would gain a disproportionate speedup, eliminating the incentive for less powerful quantum miners - as well as those who lack quantum computers entirely - to participate at all"*. Researchers suggest that this inherent flaw in all conventional PoW designs could reduce Bitcoin mining to just two dominant quantum miners[12], effectively undermining

11 Because Grover's algorithm doesn't parallelise, it's much more advantageous to have fewer, faster quantum miners than more, slower quantum miners.

12 The reason it's two miners rather than one relates to game theoretical principles where a complete monopoly is unstable in certain competitive scenarios, whereas a duopoly can reach a stable equilibrium.

the decentralized foundation that provides Bitcoin's security and censorship resistance. A solution to this specific attack has been proposed, but further research is needed to fully understand both the nature of the threat and the range of potential mitigations.

Practical Limitations of Quantum Mining

For quantum mining to evolve from theoretical concern to practical threat, significant progress will have had to be achieved; quantum mining faces substantial practical limitations that push its viability well into the future. To begin, there is likely to be a wide performance gap between classical and quantum hardware for some time. As of May 2025, there are individual ASIC miners that are capable of operating at ~500 TH/s [Bit25], with the Bitcoin network's total hash rate exceeding 800 EH/s [Mem25]. By comparison, research estimates that a quantum miner with "optimistic specifications" would achieve an effective hash rate of only about 13.8 GH/s; more than 1000x slower than a single modern ASIC [ABL+17].

The performance gap stems from several fundamental challenges. First, quantum computers are expected to initially operate at significantly slower clock rates than classical hardware. While classical circuits can operate at multiple GHz, quantum gate operations are much slower, currently limited to tens or hundreds of MHz. Second, unlike classical mining, where adding more miners directly reduces solution time proportionally, because Grover's algorithm cannot be efficiently parallelized, there is no unique advantage over ASICs when deploying additional quantum miners [QCS25].

Bitcoin mining is a highly competitive activity featuring global competition and tight margins. Accordingly, for quantum miners to participate in the market, they would need to be profitable. A quantum miner would need to have an economic advantage, which would be when a quantum miner is capable of mining blocks with a shorter expected time to mine than a comparably expensive classical miner [CMN23]. Research indicates that quantum miners would need to achieve dramatically higher energy efficiency compared to classical systems, potentially by several orders of magnitude, to become economically competitive in the mining ecosystem [NG21].

5. Post-Quantum Cryptography

Post-quantum cryptography (PQC) has emerged as the critical response to the looming threat that CRQCs pose to current cryptographic foundations. This section examines PQC, the field of cryptographic approaches believed secure against both classical and quantum computing threats, beginning with a brief examination of the properties and characteristics of the various families of PQC approaches. This leads to a consideration of NIST's PQC Standardization Process, alternative PQC approaches being pursued by China, the European Union, and other regions seeking cryptographic sovereignty, while acknowledging the legitimate trust concerns stemming from historical cases of governments compromising cryptographic standards. Industry response is then covered, with numerous technology companies having deployed hybrid solutions that combine classical approaches (such as ECC) with post-quantum algorithms in their services and products in the last few years.

Post-Quantum Cryptography

PQC refers to cryptographic algorithms and cryptosystems that are believed to be secure against attacks by both classical and quantum computers. The field developed following Peter Shor's theoretical demonstrations that a quantum computer could efficiently factor large numbers and compute discrete logarithms, breaking the foundation of much modern cryptography, using Shor's algorithm [Sho95]. Several families of post-quantum cryptographic approaches have been developed since: lattice-based, hash-based, code-based, isogeny-based, and multivariate-based cryptography.

Although the details of these different approaches are beyond the scope of this report, it's important to recognize that the approaches all vary in properties such as maturity and level of scrutiny, key sizes, signature lengths, and time required to sign and verify. And for the purpose of detailing their suitability for application to something like Bitcoin, it's important to understand how the various properties of each PQC approach measure up against the ECC-based ECDSA and Schnorr signature schemes. Table 1, adapted from BIP-360 [Bea24a] and the PQ Signatures Zoo [PQS24, WV24], summarizes a selection of quantum-resistant signature algorithms from the various families, with an emphasis on showing the size of signatures and public keys, as well as the time to sign and verify, of each approach relative to ECDSA/Schnorr.

Signature Algorithm	Year	Cryptography	Public Key Size	Public Key Size vs. Schnorr	Signature Size	Signature Size vs. Schnorr	Cost to sign vs. ECDSA	Cost to verify vs. ECDSA
Schnorr	1989	ECC	32 bytes	1.0x	64 bytes	1.0x	1.0x	1.0x
ECDSA [1]	1992	ECC	32-33 bytes	1.0x	70-72 bytes	1.1x	1.05x [2]	1.05x [2]
Lamport	1977	Hash	16384 bytes	512x	8192 bytes	117x	~0.3x [3]	~5x [3]
XMSS	2011	Hash	68 bytes	2.1x	2440 bytes	38x	~30x [4]	~50x [4]
SPHINCS+ 128s	2015	Hash	32 bytes	1.0x	7856 bytes	122x	~111,000x	~37x
SPHINCS+ 128s	2015	Hash	32 bytes	1.0x	17088 bytes	267x	~5,700x	~99x
CRYSTALS-Dilithium 44	2017	Lattice	1312 bytes	41x	2420 bytes	38x	~8x	~0.9x
FALCON 512	2017	Lattice	897 bytes	28x	666 bytes	10x	~24x	~0.6x
SQIsign I	2023	Isogeny	64 bytes	2x	177 bytes	2.8x	~135,000x	~830x

Table 1: Signature algorithm performance and size comparison relative to Schnorr. Cost to sign and verify are only indicative. Unless otherwise identified, results are from Post-Quantum Signatures Zoo [PQS24].

1 We choose to compare against Schnorr rather than ECDSA as the source [WV24] was EdDSA with 64 byte signature.

2 Schnorr will be more performant when batch validation of signatures can be utilised [BSE18b].

3 Based on required SHA-256 operations, and number of SHA-256 that can be performed on modern hardware, per cycle.

4 Based on results from [RMS25] and [OLC17].

The table reveals the general characteristics of the different families of PQC approaches. Hash-based schemes like SPHINCS+ offer extremely compact public keys but come with the largest signatures, whereas lattice-based approaches (FALCON and CRYSTALS-Dilithium) offer a more balanced tradeoff between public key and signature size. The newer isogeny-based approaches such as SQIsign show promise with the smallest signature sizes and relatively compact public keys, however, they are both relatively new, so there is much less vetting and peer review, and also significantly slower to sign and verify. Critically, one of the leading isogeny-based candidates of NIST's PQC Standardization Process, described below, SIKE, was broken in approximately 1 hour using a desktop computer in August 2022, casting doubt on the entire family of isogeny-based approaches [JAC+22, Gee23]. In general, as the trend in Table 1 indicates, cryptographic techniques tend to improve on various measures (signature size, public key size, performance-wise) as time goes on, suggesting that it is advantageous to wait for further advancements before committing to any single approach.

NIST's Post-Quantum Cryptography Standardization Process

In recognition of the long-term threat quantum computers pose to current cryptographic standards, NIST initiated its PQC Standardization Process in December 2016. This followed earlier efforts such as the PQCrypto conference series, which started in 2006 [PQC06], and various projects in the EU (PQCrypto and SAFEcrypto) and Japan (CREST Crypto-Math) [CLJ+16]. NIST's process, which has solicited algorithm submissions and the involvement of the global cryptographic community, is intended to publicly analyze, test, and standardize algorithms that are believed to be resistant to attacks from both classical and quantum computers alike. As of March 2025, NIST had finalized 3 PQC standards (FIPS 203 [NIS24a], FIPS 204 [NIS24b], FIPS 205 [NIS24c]), had advised another will be released in 2025 as draft status (FIPS 206) [NIS24d], and had indicated another candidate algorithm will be further evaluated over the next year or so, to be released as a draft in 2026 (if all goes well) [NIS25].

Of these PQC standards or proposed standards, those pertaining to digital signatures are the most relevant to address Bitcoin's CRQC vulnerabilities. These are:

- FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA), based on CRYSTALS-Dilithium.
- FIPS 205: Stateless Hash-Based Digital Signature Standard (SLH-DSA), based on SPHINCS+.
- FIPS 206: Fast Fourier Transform over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA), based on FALCON. Draft status expected in 2025.

Government Post-Quantum Initiatives and Timelines

National governments around the world are responding to the potential for significant disruption that a CRQC could cause to existing cryptographic systems by developing transition strategies to post-quantum alternatives. As of mid 2025, more than 15 countries and regions have published official guidance on PQC transitions, with many following NIST's standardization efforts while some are developing their own algorithms [GSM25]. The timeline for complete transition ranges from 2027 to 2035, with most countries targeting 2030 as a milestone year for significant progress. A few of the more significant efforts are detailed in the following.

United States

The United States has established one of the most comprehensive and detailed approaches:

- The National Security Memorandum 10 issued by President Biden in May 2022, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" sets *"the goal of mitigating as much of the quantum risk as is feasible by 2035"* [OMB22].
- NIST has set a deadline of 2030 for the deprecation of widely used RSA-2048 and ECC-256 algorithms, with a complete disallowance of their use by 2035 [MPR+24]. There's an exception made for hybrid cryptography that combines ECC and post-quantum algorithms.

Table 2: Quantum-vulnerable digital signature algorithms

Digital Signature Algorithm Family	Parameters	Transition
ECDSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035
EdDSA [FIPS186]	≥ 128 bits of security strength	***Disallowed*** after 2035
RSA [FIPS186]	112 bits of security strength	***Deprecated*** after 2030 ***Disallowed*** after 2035
	≥ 128 bits of security strength	***Disallowed*** after 2035

- The National Security Agency's (NSA) 'Commercial National Security Algorithm Suite (CNSA) 2.0' has established a timeline for software and networking equipment to be upgraded by 2030, with browsers and operating systems fully upgraded by 2033 [NSA22].
- Executive Order 14144, issued in January 2025, 'Strengthening And Promoting Innovation In The Nation's Cybersecurity', further strengthened implementation requirements and directs the engagement of *"foreign governments and industry groups in key countries to encourage their transition to PQC algorithms standardized by NIST"* [EOP25].

United Kingdom

The UK's National Cyber Security Centre (NCSC), which is part of Government Communications Headquarters (GCHQ), issued guidance in March 2025 to help the nation

prepare for and protect against threats posed by future developments in quantum computing with three phases for migration [NCS25]:

- To 2028 – identify cryptographic services needing upgrades and build a migration plan.
- From 2028 to 2031 – execute high-priority upgrades and refine plans as PQC evolves.
- From 2031 to 2035 – complete migration to PQC for all systems, services, and products.

The UK's migration framework is built around the anticipated acceptance of NIST standards as they are incorporated into protocols through bodies like the Internet Engineering Task Force (IETF).

European Union

The EU has its own approach to post-quantum cryptography coordinated by the European Telecommunications Standards Institute (ETSI) through its Quantum-Safe Cryptography (QSC) working group established in 2015 [ETS15, PQC15]. ETSI has introduced its own guidelines for migration to quantum-safe schemes [ETS20] and a standard for key establishment [ETS25], though it has also released technical reports to support NIST standards for PQC [ETS21]. The EU and ETSI have not yet established timelines advising of or mandating PQC adoption.

China

China is pursuing a more independent and sovereign approach to PQC than most other countries. Rather than adopting NIST standards, China launched its own "Next-generation Commercial Cryptographic Algorithms Program" (NGCC) in February 2025 through the Institute of Commercial Cryptography Standards [ICC25]. It is doing so to create home-grown PQC algorithms that align with its national cryptographic standards and security requirements, wishing to emphasize technological self-reliance in this domain. No specific implementation timeline has been publicly announced.

Following Government Standards on Post-Quantum Cryptography

NIST, which is part of the U.S. Department of Commerce, has been globally influential in the standardization of cryptographic systems for many decades. Beginning with the introduction of the Data Encryption Standard (DES) in the 1970s, NIST has been responsible for standardising secure hash standards, SHA-1 (1995), SHA-2 (2001), SHA-3 (2015), Advanced Encryption Standard (AES, 2001), key management schemes, Random Number Generation (RNG) systems, block cipher modes of operation, password-based key derivation (PBKDF2, 2010), authenticated encryption schemes and, of course, elliptic curve cryptography (ECC). All are used in countless cryptographic systems worldwide.

Although NIST has traditionally been viewed by many to be a trustworthy organization for cryptographic standards, this trustworthiness was brought into disrepute in 2013 with the

Snowden revelations. These disclosures confirmed that at least one NIST standard (Dual_EC_DRBG) contained a backdoor deliberately engineered by the NSA, raising concerns about potential NSA influence over other NIST standards [FBS+23]. This context is particularly relevant when considering Bitcoin's use of non-NIST cryptographic primitives like the secp256k1 curve, and when evaluating whether to follow NIST's PQC recommendations for future changes to Bitcoin.

Not all entities are intending to follow NIST standards on PQC, either completely or without additional independent evaluation. It is likely that China's decision to pursue independent cryptographic standards is at least partially motivated by concerns over potential backdoors that could allow U.S. intelligence agencies to access encrypted information [Spa25].

The EU, through ETSI, is taking a complementary but somewhat independent path, creating standards that address European regulatory requirements while maintaining compatibility with global systems. Several countries, including South Korea, Japan, and the Netherlands, are adopting hybrid approaches that implement both NIST-recommended algorithms and supplementary algorithms from national research initiatives [GSM25].

For Bitcoin specifically, the emergence of multiple independent PQC approaches presents a potential opportunity rather than a challenge. Bitcoin's security model already benefits from relying on cryptographic primitives that were not developed by government agencies, notably the adoption of secp256k1 curve, which was developed by the Standards for Efficient Cryptography Group (SECG), rather than using any NIST curves. A competitive environment with multiple PQC alternatives could allow the Bitcoin community to evaluate different approaches based on their technical merits, security properties, and performance characteristics, potentially adopting solutions that best align with Bitcoin's unique requirements (and are least likely to be compromised in some way).

Post-Quantum Cryptography in Industry

Some notable companies that rely on cryptography as part of their service or product offering have already made the transition to PQC. In October 2022, Cloudflare announced that "all websites and APIs served through Cloudflare support post-quantum hybrid key agreement" [WR22]. Their design, which combines traditional ECC with the post-quantum Kyber algorithm, requires an attacker to break both encryption techniques in order to break the hybrid scheme.

In August 2023, Google announced that its Chrome browser would begin supporting hybrid key generation mechanisms similar to those adopted by Cloudflare the year prior [OBr23]. Google said *"the sooner we can update TLS to use quantum-resistant session keys, the sooner we can protect user network traffic against future quantum cryptanalysis"*, referencing the **harvest now, decrypt later** attack whereby encrypted data is collected and stored today, to be decrypted later once CRQCs are available.

Shortly afterwards, in September 2023, Signal, a leading privacy-focused messaging app, announced that they had added a *"layer of protection against the threat of a quantum computer being built in the future that is powerful enough to break current encryption standards"* [Kre23]. Signal also opted to augment their existing ECC-based cryptosystems with the CRYSTALS-Kyber post-quantum key encapsulation.

In February 2024, Apple announced that they had designed a new cryptographic protocol for iMessage, PQ3, [ASE24]. This protocol features PQC being used to *"secure both the initial key*

establishment and the ongoing message exchange, with the ability to rapidly and automatically restore the cryptographic security of a conversation even if a given key becomes compromised". Other companies are likely to follow suit as PQC continues to move towards becoming an industry standard.

6. Post Quantum Bitcoin

The Bitcoin community has been aware of the quantum threat since Bitcoin's early days and has been discussing various approaches to address post-quantum security for over a decade. This section examines efforts within Bitcoin to implement PQC and explores the fundamental philosophical and practical challenges of transitioning Bitcoin to post-quantum security, including the question of what to do with quantum-vulnerable funds and the scale of potentially affected Bitcoin holdings. Similar initiatives in other cryptocurrencies are also briefly detailed.

Post-Quantum Cryptography Efforts in Bitcoin

Recognizing that CRQC private key derivation and the forging of signatures pose a severe risk, several public initiatives have emerged to address post-quantum security for Bitcoin. These initiatives range from the discussion and debate between members of Bitcoin's development community on mediums such as the BitcoinTalk forum [BT], the Bitcoin Development Mailing List (BDML) [BDML] and the Delving Bitcoin forum [DBF] through to PQC change proposals for Bitcoin such as BIP-347: OP_CAT potentially enabling Lamport signatures [HS23], the introduction of a post-quantum signature verification opcode for quantum-secure Taproot scripts [Cor24], and a new script type, P2QRH with BIP-360: Pay to Quantum Resistant Hash [Bea24a, Beas24b].

Early Post-Quantum Cryptography Efforts in Bitcoin

Most of the early post-quantum cryptography efforts in Bitcoin were confined to discussions, rather than any concrete development effort[13]. Discussions were primarily focused on replacing ECC (due to security concerns, see Following Government Standards on Post-Quantum Cryptography) and switching away from SHA-256 were it to be broken. Satoshi's only public comment on the matter is from 2010 and related to the breaking of SHA-256:

"SHA-256 is very strong. It's not like the incremental step from MD5 to SHA1. It can last several decades unless there's some massive breakthrough attack.

If SHA-256 became completely broken, I think we could come to some agreement about what the honest block chain was before the trouble started, lock that in and continue from there with a new hash function.

If the hash breakdown came gradually, we could transition to a new hash in an orderly way. The software would be programmed to start using a new hash after a certain block number. Everyone would have to upgrade by that time. The software could save the new hash of all the old blocks to make sure a different block with the same old hash can't be used." [Nak10]

13 Though Greg Maxwell in 2013 stated having a Lamport implementation *"that I've been sort of sitting on in case of cryptographic doomsday"* that he developed a few years prior [Max13a].

Lamport signatures were initially proposed as a construction that could replace ECC [Max13b], as they are historically and widely regarded to be resistant to CRQC attacks [CSE13]. However, there are caveats, including that they are a one-time signature scheme, so signing more than once with a public key reveals information about the secret key [But13], and that *"they are horribly inefficient, taking multiple kilobytes of data for both keys and signatures"* [Poe24] in being about ~120x the size of a comparable ECDSA or Schnorr signature (see Table 1). An extension to Lamport signatures, the Merkle signature scheme, was identified as perhaps a more appropriate alternative construction in that it permitted key re-use [Wik13].

Lamport and Merkle signature schemes, like the more modern SPHINCS+ standardized by NIST in FIPS-205, are examples of hash-based methods. Hash-based methods have received the most evaluation and scrutiny of all the PQC approaches, as such, although they are inefficient as described, there is significant confidence amongst the cryptographic community in their security against both classical and quantum attacks.

Lamport Signatures with OP_CAT, Quantum-Secure Taproot Scripts

The proposed reintroduction of OP_CAT by Ethan Heilman and Armin Sabouri with "BIP-347: OP_CAT in Tapscript" is, in part, motivated by enabling post-quantum Lamport signatures in Bitcoin transactions [JRCAT]. This is because all that is required to create Lamport signatures is the ability to hash and concatenate values on the stack, with concatenation being the missing piece that OP_CAT enables. In a blog post titled "Quantum Proofing Bitcoin with a CAT" Jeremy Rubin notes: *"Fun Fact: OP_CAT existed in Bitcoin until 2010, when Satoshi 'secretly' forked out a bunch of opcodes. So in theory the original Bitcoin implementation supported Post Quantum cryptography out of the box!"*[14].

BIP-347 points out that with OP_CAT enabling the creation of Lamport signatures, users could *"mark their Taproot outputs as 'script-path only' and then move their coins into such outputs with a leaf in the script tree requiring a Lamport signature"* [HS23]. This would build upon the dual-spending mechanism of Taproot, where it's possible to spend Taproot outputs via either the key-path, with a single valid signature from the designated public key, or the script-path, which supports alternative spending conditions such as this Lamport construction.

Reintroducing OP_CAT (via soft fork) would allow wallets to construct Taproot outputs that contain a script-path encapsulating a Lamport signature spending condition. Because of the vulnerability of exposed public keys in the Taproot key-path as described in Immediately Vulnerable Script Types, it would also be necessary for the Taproot key-path spend to be disabled when quantum computers are a reality, such that spends could only occur by the script-path.

One of the major drawbacks, aside from the very large key and signature sizes of Lamport signatures, is that the only way to disable Taproot key-path spends is with a soft fork, thus

14 Satoshi disabled OP_CAT and 15 other opcodes purportedly due to exponential stack element growth risks [HS23]. This is no longer a concern since Tapscript now enforces a 520-byte maximum stack element size.

two soft forks are likely required for full quantum security via the OP_CAT approach. OP_CAT is also motivated by more than just Lamport signatures and could be used in a variety of other use cases, but its introduction could expand Bitcoin's attack surfaces *"since it's impossible to predict all the consequences of activating OP_CAT we cannot confidently assert its safety"* according to Robin Linus [Lin24].

A similar idea was put forward by Matt Corallo on the BDML under "Trivial QC signatures with clean upgrade path" where he proposed the addition of an OP_SPHINCS or equivalent post-quantum non-one-time-use signature verification opcode [Cor24]. The inclusion of such an opcode would allow wallets to construct Taproot script-path outputs that are a quantum-secure path, similar to the Lamport signature spending condition built with OP_CAT, but via a dedicated opcode rather than building on OP_CAT.

Although it was thought to require a soft fork, Luke Dashjr suggested that this isn't strictly necessary as long as there is a well-defined quantum-secure script to build against and then *"wallets could begin implementing this fallback immediately, without waiting for any soft fork activation, as soon as the spec is final"*. The idea to start implementing against a standard SPHINCS implementation today was contended by Anthony Towns *"adding in secret OP_SPHINCS spend paths prior to an OP_SPHINCS consensus change being active (or at least locked-in) seems very risky"*.

Despite this and other implementation debates, Corallo's fundamental point is that providing an optional quantum-resistant pathway now, whether via OP_CAT or via a dedicated quantum-resistant signature verification opcode, could significantly reduce the volume of vulnerable coins compared to waiting until quantum threats are imminent. As Corallo notes, *"if we give wallets a decade or a decade and a half of time with a PQC option then the total funds vulnerable to theft could be substantially decreased"*.

BIP-360: QuBit - Pay to Quantum Resistant Hash

In September 2024, Hunter Beast (cryptoquick) opened "BIP-360: QuBit - Pay to Quantum Resistant Hash", the culmination of *"several months gathering feedback from the mailing list and from other advisors"* [Bea24a]. BIP-360 proposes the introduction of a new output type, Pay-to-Quantum-Resistant-Hash (P2QRH), that relies on NIST PQC signature algorithms. The proposed mechanism for introducing this post-quantum secure output type, P2QRH, is via soft-fork.

P2QRH leverages P2TR by combining classical Schnorr signatures with PQC signatures in a hybrid approach. A significant difference between the current SegWit version 1 P2TR and the proposed P2QRH is that, rather than having an exposed public key as with P2TR, a hash (using HASH256) of the public key will be used. Being a major deviation from P2TR, a new SegWit version, version 3, is proposed - *"this results in addresses that start with bc1r, which could be a useful way to remember that these are quantum (r)esistant addresses"*.

In recognising that there is no PQC signature algorithm that is a clear standout choice, BIP-360 currently proposes the 3 PQC signature algorithms that are favoured by NIST:

- FN-DSA-512 - FIPS 206 - FALCON-512
- ML-DSA-44 - FIPS 204 - CRYSTALS-Dilithium Level I
- SLH-DSA-SHAKE-128s - FIPS 205 - SPHINCS+-128s

The BIP acknowledges, as detailed in Post-Quantum Cryptography, that implementing quantum-resistant signatures and public keys would likely increase transaction sizes significantly compared to current ECC-based methods. This increased size would consume more block space, consequently affecting transaction fees and reducing overall network throughput.

While BIP-360 is probably the furthest along of all the approaches examined, the proposed changes are still far from being accepted. Mark Erhardt (murch) summarizes the sentiment with *"there seem to be concerns about e.g., introducing too many different PQ Signature schemes introducing unnecessary complexity, the resulting scheme dropping support for existing features, and uncertainty about the properties of the attestation structure's properties"*. However, Ethan Heilman, a co-author of the BIP, is planning to explore incorporating script paths and revisiting the use of multiple signatures to enhance the proposal's flexibility in future iterations.

In a response to a BIP-360 thread on the BDML, Jonas Nick highlights that *"all new cryptographic schemes added to the consensus protocol need be exceptionally well specified and implemented"* regarding the introduction of multiple different post-quantum schemes [Nic25]. Although there's some perception that the focus should be on specifying a single signature algorithm, it should be noted that the rationale for the inclusion of multiple schemes is one of risk mitigation, were any of the specified PQC schemes to be broken. Ethan Heilman contends that supporting two signatures is the most rational approach. He suggests using FALCON, which has widespread adoption potential with good size and performance, alongside SPHINCS+, a widely trusted but less efficient alternative that serves as a security fallback.

There's also some uncertainty around whether scripting in outputs still works with the proposal. Mark Erhardt's question of *"don't we still want HTLCs in a PQ future?"* is answered with *"I expect this to be compatible with a lot that's already been developed for Lightning and Taproot. I would like to verify that in practice however"*. On the BDML, concerns about the possibility of the attestation structure being used to include arbitrary data are raised. In a response to the various BIP-360 feedback, Hunter Beast states that *"there's too many variables to consider without something concrete to work from and think about"* suggesting that BIP-360 (and the associated `libbitcoinpqc` codebase [Bea25b]) is a proving ground for experimentation and practical validation, positioning it as a starting point for Bitcoin's quantum-resistant evolution rather than a final solution.

Other Post-Quantum Cryptography Efforts in Bitcoin

The significant size of post-quantum public keys and signatures relative to current public keys and sizes is a problem that is referenced in almost all post-quantum Bitcoin discussions. To address this issue, BIP-360 proposes a "quantum witness" - witness or attestation data for post-quantum public keys and signatures. This quantum witness would receive a witness discount in a similar manner to the witness discount of witness data in a SegWit transaction. BIP-360 states *"... to maintain present transaction throughput, an increase in the witness discount will likely be desired in a QuBit soft fork. That will be specified in a future QuBit BIP".*

While this witness discount approach could indeed result in an unchanged number of transactions per block as compared to what is currently possible, the underlying transaction

and block data will be significantly larger with post-quantum public keys and signatures. A recent suggestion by Ethan Heilman on the BDML proposes an alternative involving compressing transaction data of transactions supporting post-quantum signatures such that there is a single structure, a Scalable Transparent ARguments of Knowledge (STARK), representing the validity of all aggregated signatures [Hei25]. The resultant STARK, a single compact proof, would verify transaction validity while hiding the specific signature details, thus maintaining privacy and reducing block space requirements.

This approach could transform Bitcoin's scaling dynamics: according to Heilman's calculations, compressing post-quantum signatures with STARKs could reduce transaction sizes and increase effective throughput by an order of magnitude on what is possible today. Beyond improved throughput, this method would fundamentally alter the economics of on-chain transactions by making payment usage significantly more affordable relative to data storage uses. It may also drive greater adoption of privacy techniques such as coinjoins and payjoins, as transactions would be cheaper when part of an aggregated proof.

But there are still many details to be debated and discussed for the idea to gain further traction. Key concerns include transaction and block relay protocols, the impact on mining decentralization from STARK computation requirements, the integration of new security assumptions into Bitcoin's consensus rules, and the development of supporting wallet infrastructure. This approach, while undoubtedly innovative, introduces considerable complexity compared to simpler post-quantum alternatives, such as just using hash-based signatures, so it would certainly require significant community engagement.

Beyond these public proposals, research is being conducted by several leading cryptographers and Bitcoin developers. Individuals including Tim Ruffing and Jonas Nick, who have been involved with the design and development of critical improvements like Schnorr signatures, Taproot, and MuSig2, are now applying their expertise to Bitcoin's quantum resistance challenges. Involvement of individuals who have established track records in research culminating in significant change in Bitcoin will be essential as post-quantum solutions progress from theoretical research to practical implementation proposals. Their ongoing work, while sometimes less visible than public discussions, represents essential cryptographic and engineering groundwork toward Bitcoin's quantum-secure future.

These initiatives and ideas are important steps, yet they represent just the beginning - the landscape of possibilities extends far beyond current proposals. As the community experiments with different cryptographic techniques and approaches, it's expected that new solutions promising a better balance between security, efficiency, and compatibility will emerge. While these solutions will be carefully evaluated and debated by the community, Bitcoin's increasingly diverse ecosystem makes consensus-building more challenging than in previous upgrade efforts. Nevertheless, as outlined in Short-Term Contingency Measures, when faced with imminent threats, Bitcoin has demonstrated capacity for accelerated decision-making through coordinated action, and when CRQCs begin to pose a credible threat to Bitcoin, this existential risk would likely catalyze similar urgency, compelling stakeholders to unite to preserve Bitcoin's security and value proposition.

Philosophical Dilemma: Burn vs. Steal

If it is accepted that CRQCs will one day be a reality, perhaps the most difficult decision facing the Bitcoin community is what should be done, if anything, about all of the UTXOs that are currently vulnerable with exposed public keys (quantum-vulnerable). The question is:

Should quantum-vulnerable funds be made unspendable, or should they be left available for recovery by quantum computers?

This represents a fundamental philosophical decision point as it encapsulates questions of Bitcoin's foundational values, such as property rights, censorship resistance, forward compatibility, and conservatism.

It is argued by some that making quantum-vulnerable funds unspendable - "burning" the UTXOs - best preserves Bitcoin's integrity as a system designed to protect property rights. As Jameson Lopp articulated in his "Against Allowing Quantum Recovery of Bitcoin" opinion piece [Lop25a] (and also on the BDML [Lop25b]), allowing quantum computers to claim these funds would amount to a form of wealth redistribution from those who lost access to their coins to those who win the technological arms race to acquire quantum computers. The burn approach essentially treats quantum vulnerability as a protocol-level bug that requires a conservative fix, much like previous vulnerabilities that have been patched to protect the network.

To the contrary, others take the position that burning quantum-vulnerable funds would be confiscatory and would violate the property rights of their owners - *"not freezing user funds is one of Bitcoin's inviolable properties"*. Proponents of this perspective argue that Bitcoin was designed as a system where users maintain complete sovereignty over their funds, with the freedom to access them whenever they choose. By making certain UTXOs unspendable, the network would effectively be seizing control from rightful owners who may simply be unaware of the quantum threat or unable to migrate their coins in time. For such entities, a protocol change that renders their funds permanently inaccessible would represent precisely the kind of third-party intervention that Bitcoin was created to prevent.

If a "burn" approach is adopted, the total supply of Bitcoin would effectively decrease, potentially increasing the value of the remaining coins. Conversely, if vulnerable funds remain open for "stealing" by quantum computers, the Bitcoin ecosystem faces the prospect of a significant redistribution of wealth to the first entities with sufficient quantum computing capabilities. A coordinated "burn" process or event would provide a degree of certainty around timelines and may limit market volatility, whereas the gradual and prolonged "stealing" of vulnerable funds might create sustained market volatility, which could have many downstream effects given the level of financialization now involved with Bitcoin.

A decision to adopt the "burn" approach also necessitates considerations and decisions on exactly what funds (UTXOs) should be burnt, how this information is to be disseminated, what transition period would be appropriate, and how the burn is enforced or implemented. A decision to burn could also have legal implications, so there may need to be legal protections or guarantees for those individuals involved in enacting "the burn".

There is much less to consider for the "steal" approach, as the steal path is effectively the "do nothing" option. This approach may reward entities that develop quantum computing technology with a windfall of bitcoin, regardless of their contribution to the network itself. And there could be legal implications if nothing is done when CRQCs appear to be a certainty – if a quantum attacker gains access to and spends someone's UTXOs, would members of the Bitcoin community be liable in some way?

The debate and discussion on this matter is still ongoing, with an increasing number of individuals and entities engaging and providing their thoughts across many different mediums. It seems imperative that many, if not all, of the outstanding considerations should be largely resolved by the Bitcoin ecosystem before a decision on burn vs. steal can be made.

Size and Ownership of Quantum-Vulnerable Funds

Quantifying the scale and distribution of quantum-vulnerable Bitcoin is essential for understanding the risk landscape, as the concentration of vulnerable funds creates an uneven risk profile with implications for prioritizing protective measures. Estimates vary from about 25% of the current supply (just over 4 million BTC) [BBH] to upwards of 50% (almost 10 million BTC) [Wui19], with some more precise estimates suggesting 6.26 million (~30%) [PE25] being immediately quantum-vulnerable (other funds are predicted to become vulnerable for a short period of time upon spend). The immediately vulnerable holdings can be categorized into several groups:

- **Satoshi-era holdings**: Estimated at between 600K and 1.1 million BTC [RR17]. These earliest mined coins remain in legacy P2PK addresses with fully exposed public keys, making them inherently quantum-vulnerable. Despite representing 3-5.5% of Bitcoin's current supply, these coins have remained untouched since they were mined in 2009-2010, leading many to speculate they may never be moved.
- **Lost coins**: A substantial portion of vulnerable funds likely belongs to users who have lost access to their private keys. Estimates based on on-chain analysis put the figure at between 2-3 million BTC in 2017, though not all lost coins would be quantum-vulnerable [RR17].
- **Public key exposed**: As mentioned previously, address re-use leads to the possibility of exposed public keys when a UTXO of some address has been spent, yet other UTXOs remain at the same address. Project 11 reported that, as of mid January 2015, there were ~11.1 million BTC addresses with a non-zero balance and exposed public key for ~6.26 million BTC [PE25].

Satoshi-era holdings, while substantial in aggregate, consist primarily of thousands of individual 50 Bitcoin P2PK UTXOs from early mining efforts. It's also impossible to know if funds identified as being lost are really lost[15], as the determination of "lost" is primarily based on age and transaction activity (excluding the early mined Satoshi-era coins). The truly lost

15 During the "Kleiman v. Wright" court case in 2020, the keys corresponding to 145 addresses that had not transacted since 2009 were used to sign messages to prove ownership, demonstrating that these funds were simply dormant, not lost.

coins are likely to be in UTXOs of varying size and script type, with only some portion being quantum-vulnerable. These Satoshi-era holdings and coins that are truly lost and quantum-vulnerable are in some sense permanently exposed to quantum attack, as they cannot be moved by their owners to more quantum-resistant script types.

Regarding public key exposed holdings, many large holders, including exchanges and institutional custodians, have historically managed their cold storage using address reuse patterns for operational simplicity, while some continue to do so. The other major avenue for public key exposure is when there has been a spend on a fork like Bitcoin Cash or Bitcoin Gold, but remains as a UTXO on Bitcoin (the address has otherwise not been reused on Bitcoin) [SIZ+18]. Public key exposed holdings represent a manageable quantum vulnerability, as owners retain the ability to transfer these funds to quantum-resistant script types when necessary.

Exchange and institutional holdings that fall into this category of vulnerability due to exposed public keys often exist as a small number of high-value, identifiable addresses, creating a concentration of quantum-vulnerable funds[16]. This creates an economic priority list for potential quantum attackers - high-value, exposed addresses would provide attackers with the maximum return for time and effort invested. This concentration of risk has practical implications for any mitigation strategy, as these high-value vulnerable addresses represent the most urgent security concern, yet may be controlled by a small number of stakeholders (relative to the size of the Bitcoin community).

Post-Quantum Cryptography in Other Cryptocurrencies

There are a handful of minor cryptocurrencies that utilize quantum-secure signature schemes, including Quantum Resistant Ledger, which uses hash-based one-time Merkle-tree Signature Scheme (XMSS) instead of ECDSA, and IOTA, which uses the Winternitz One-time Signature Scheme (WOTS), also a hash-based approach.

The most coordinated activity is probably occurring within the Ethereum ecosystem, with the Ethereum Foundation paying the salaries of many researchers and otherwise funding many avenues of research. While a detailed treatment of these Ethereum Foundation initiatives is beyond the scope of this report, the lines of research to integrate post-quantum security into Ethereum include investigating adoption of Falcon-based “smart wallet signatures” (replacing ECDSA), use of variants of XMSS to replace BLS signatures in Ethereum’s proof-of-stake consensus, and how to unilaterally hard-fork to save most users’ funds in a quantum emergency [But24].

16 Some contain tens or hundreds of thousands of Bitcoin, as is evident from the Bitcoin Rich List [BIC25].

7. Migration Pathways Overview

Transitioning the Bitcoin ecosystem to PQC presents one of the most consequential undertakings in the history of Bitcoin. While quantum-resistant signatures could be introduced to Bitcoin Core once technical consensus is reached, effectively orchestrating the migration of millions of UTXOs to quantum-resistant scripts may require unprecedented coordination across the entire network. This section examines the practical aspects of how such a transition could proceed, including the required blockchain resources and mechanisms for migration, as well as key considerations like activation methods, stakeholder education, and coordination. Understanding the migration pathways is essential for all Bitcoin holders so that they can begin to develop appropriate risk management strategies as quantum computing capabilities continue to advance.

UTXO Migration

As of May 2025, the size of Bitcoin's UTXO set is approximately 190 million UTXOs. Only a subset of these UTXOs are vulnerable to long-range attacks with exposed public keys, yet all are vulnerable to short-range attacks when they are spent in a transaction and before (or shortly after) the transaction is confirmed, as described in On-Spend Vulnerable Script Types. As such, in the ideal case, all UTXOs would migrate to quantum-resistant scripts, that is, they would be spent to create new UTXOs that are based on quantum-resistant signatures. In a practical sense, only a subset of the UTXOs are available to be migrated due to some being inaccessible (e.g., lost keys); these inaccessible UTXOs are subject to The Philosophical Dilemma: Burn or Steal. Even so, migrating even a significant portion of these funds would challenge the Bitcoin blockchain resource constraints.

Research from 2024 attempted to qualify the time required to migrate, calculating that it would take approximately 76 days, assuming the migration of all UTXOs, 100% of block space dedicated to migration transactions, and various other assumptions around theoretically optimal migration blocks [PKM+24]. Other estimates to migrate the full UTXO set with 100% block space utilization put the migration at 142 days [Lop24].

In more realistic scenarios where migration competes with regular transaction activity, the timeline extends considerably. If 25% of block space were allocated to migration transactions, migration would require, based on the above ranges, 305 to 568 days to complete. It's worth also noting that regular transaction activity on the network would likely adopt quantum-resistant scripts as a matter of necessity, and that only the accessible, exposed public key UTXOs would need to be migrated with some urgency. It may also be possible to improve on these estimates with optimizations such as transaction batching and (not currently possible but under discussion) signature aggregation [Jah25, CT10], but ultimately, the block size and block interval are fundamental constraints that will impact any UTXO migration effort.

Migration Mechanisms

Several approaches have been proposed to facilitate the secure migration of UTXOs to quantum-resistant scripts, each making different tradeoffs between user involvement,

network enforcement, and implementation complexity. It's important to note that the migrated mechanisms detailed in the following represent current thinking, but as the design space is large, it's likely that approaches offering more elegant solutions with fewer compromises will emerge in due course.

Commit-Delay-Reveal Protocol & Variants

The Commit-Delay-Reveal (CDR) protocol was proposed in 2018 [SIZ+18], with variants having been independently proposed in the same year on Twitter by Adam Back (referencing Johnson Lau) [Bac18] and on the Bitcoin Development Mailing List by Tim Ruffing [Ruf18]. A variant, known as Guy Fawkes Signature Scheme, was also discussed on BitcoinTalk as early as 2013 [JL213] and featured in the Fawkescoin "cryptocurrency using no public-key cryptography" research proposal[17] [BM14].

CDR "*allows users to securely move their funds from old (non-quantum-resistant) outputs to those adhering to a quantum-resistant digital signature scheme*". It's a three-stage process primarily intended to assist in the migration of non-quantum-resistant outputs such as P2PKH that do not have exposed public keys, even if ECC has already been compromised. It is assumed that a quantum-resistant signature scheme has already been agreed upon and deployed (via soft fork), with CDR also requiring a soft fork to change consensus rules.

In this approach, a user first creates a commitment transaction that references one or more UTXOs that the user wants to migrate to quantum-resistant protection. This commitment transaction involves combining the vulnerable public key (of the UTXO) with a quantum resistant public key, hashing the combination, and storing the hash (the commitment) in a transaction output using OP_RETURN. The transaction would be valid under current Bitcoin rules and would be processed and included in the blockchain like any other transaction. The soft fork changes would add consensus rules that treat these commitments as binding, restricting the future movement of the committed funds to only those transactions that can demonstrate knowledge of both keys used in the original commitment.

After the commitment transaction is confirmed, the protocol enforces a mandatory delay period during which the committed funds remain unusable. The delay is a security measure to ensure that even if a CRQC capable of breaking ECC is available when the keys are revealed, an attacker couldn't reorg the blockchain far enough back to substitute an alternative fraudulent commitment. Once the security period has lapsed (a period of 6 months is proposed), the user can initiate the reveal phase by creating a transaction that consumes the UTXOs referenced in the commitment and reveals both public keys (the original ECDSA or Schnorr key and the quantum-resistant key). This reveal transaction must be signed with the quantum-resistant private key and provide proof that the revealed keys match the hash stored in the original commitment.

The CDR protocol is a conservative approach that prioritizes security with the delay phase, but does require user involvement in the commit and reveal phases. It thus can't be used to migrate all quantum-vulnerable funds, only those that can still be signed for and also don't yet

17 Fawkescoin proposed utilising the distributed consensus mechanism of Bitcoin but replacing Bitcoin's ECDSA signatures with hash-based Guy Fawkes signatures for transactions.

have revealed public keys. A significant downside is that the approach requires that, for a user to create the initial commitment transaction, they must do so from quantum-resistant funds: they *"will have to either already possess, or acquire through trade, some quantum-resistant currency units - sufficient to fund the creation of an OP_RETURN on the blockchain"*. As the approach is transaction-based, the aforementioned constraints of limited block space and block interval apply. The scheme also likely requires two soft forks, assuming a quantum-resistant signature scheme is introduced at an earlier date.

Recognizing the practical limitations of the original CDR approach, enhanced variants have been proposed to address its shortcomings. Notably, the Lifted FawkesCoin protocol solves the critical bootstrapping problem where users need post-quantum funds to pay commitment fees [SW23]. The protocol achieves this through "signature lifting," where users create zero-knowledge proofs using the post-quantum PICNIC signature scheme demonstrating they possess the private key corresponding to a public key that hashes to their address, without ever revealing that quantum-vulnerable public key. Since addresses other than P2PK, P2MS, and P2TR contain only hashes of public keys or scripts, CRQCs would need to leverage Grover's algorithm to reverse the hash functions to discover the original public key(s), and would not be able to forge the post-quantum proof.

For HD wallets, users can prove knowledge of master seeds that generate specific address hashes, enabling recovery even when individual private keys are lost, extending protection to practically all Bitcoin created since HD wallets became standard [Wui12]. However, the proposal would require consensus on integrating relatively novel zero-knowledge proof systems, representing a significantly larger departure from Bitcoin's current cryptographic primitives than simpler CDR variants.

Quantum-Resistant Address Migration Protocol

The Quantum-Resistant Address Migration Protocol (QRAMP) is a proposal that exists at the other end of the migration spectrum [Cru25]. It's a more assertive approach compared to the opt-in nature of the CDR protocol in that it proposes enforcing a mandatory migration period with a hard deadline after which UTXOs secured by ECC would become unspendable - a strict realization of the "burn" position with a "flag day" (see Quantum Canaries for an alternative to a specific date). The premise is that proactive, network-wide migration is necessary to prevent catastrophic security breaches once quantum computing advances sufficiently.

QRAMP prioritizes network security over individual autonomy by implementing a clear timeline for migration. Users would be given a substantial notice period to transfer their funds from vulnerable addresses to quantum-resistant ones. The proposal acknowledges the risk of funds being permanently locked if owners fail to migrate before the deadline, but weighs this against the potentially greater systemic risk of allowing vulnerable addresses to remain accessible indefinitely. The primary advantage of QRAMP is its unambiguous enforcement mechanism, which eliminates the complexity of transitional transaction types and provides certainty about the network's security posture after the migration deadline.

QRAMP faces significant challenges in achieving consensus as the proposal effectively necessitates the confiscation of unmigrated funds, which runs counter to Bitcoin's ethos of user sovereignty. It's also proposed to activate via a hard fork, the concept of this alone is controversial enough. Additionally, the limited block space would likely lead to a spike in fees

and transaction congestion as the deadline approaches. Some community members have suggested a more gradual approach that would initially only disable the most vulnerable script types, such as those vulnerable to long-range attack, while preserving spending capabilities for the other script types as they already offer some inherent quantum resistance in their un-reused state, for them to be disabled at a later date.

Hourglass Strategy

An alternative migration mechanism that aligns with the "steal" position is the hourglass or gating strategy. The idea is that *"rather than attempting to ban quantum attackers from spending exposed Bitcoin, we should slow the rate at which these vulnerable UTXOs can be claimed"* [Lil25] by, for example, allowing only one quantum-vulnerable spend per block[18] [Bea25a]. The hourglass strategy is promoted as a market-driven approach that would create fee competition among attackers, potentially generating substantial miner revenue over decades. This is in contrast to what could be a relatively sudden shock were the transacting of vulnerable coins to remain unrestricted.

Proponents of the hourglass strategy assert that the approach is a pragmatic recognition that miners ultimately follow economic incentives rather than ideological mandates. They believe it could strengthen Bitcoin's network security, and could potentially be an important component of the mining reward after the block subsidy ends in 2140 if quantum-vulnerable spends are suitably rate limited. Critics argue that it establishes a precedent that, under certain conditions, the network will permit the transfer of funds without the original owner's legitimate authorization. The approach could also introduce centralization risks through enforcement of rate-limiting rules. Like other proposals, the hourglass strategy would require a soft fork implementation with network-wide consensus, and it might face opposition in the community due to its explicit accommodation of coin theft rather than prevention.

Private Transaction Services

Private transaction services represent a potentially complementary or orthogonal migration strategy that specifically addresses short-range attacks during the window of vulnerability between transaction broadcast and confirmation. These services, such as existing private mempools like MARA's Slipstream [MDH24], allow users to submit transactions directly to trusted miners rather than broadcasting them publicly, preventing quantum adversaries from observing and hijacking transactions before confirmation. While this approach doesn't eliminate the need for protocol-level quantum-resistant signature schemes, it could reduce, but not eliminate[19], risks during the transition period after such schemes are implemented. It's worth noting that even today, such services are contentious in the community as they are often leveraged to include non-financial data storage transactions in the blockchain, and they create a two-tier system for transaction broadcast.

18 Hourglass also prevents the creation of any new vulnerable outputs, so each time a vulnerable output is spent, the set of vulnerable outputs decreases by one.

19 Users need to trust that such services would not use a CRQC to steal their funds.

Quantum Canaries

Quantum canaries are not a migration mechanism, but a proactive detection system for monitoring quantum computing advancement and correspondingly enacting migration procedures [Dra18]. Inspired by the practice of miners carrying canaries into mines to detect deadly gases, quantum canaries involve creating bounties on the blockchain that are locked behind quantum-solvable challenges. These challenges would be calibrated to be solvable by CRQCs significantly less powerful than those required to compromise Bitcoin's elliptic curve cryptography [SW23]. When a canary bounty is claimed, it signals to the entire network that quantum capabilities have reached a certain level, providing the community with a clear, on-chain signal to begin migration procedures. This approach creates an incentive structure where quantum-capable entities are motivated to claim the bounty rather than waiting to develop more powerful capabilities for stealing coins outright.

Soft Fork Activation Methods

Most of the proposed migration mechanisms require consensus rule changes implemented via soft fork, and are also predicated on quantum-resistant signatures having already been activated on Bitcoin (via soft fork). The level of agreement on the way forward will likely dictate which activation method is adopted. If there is a general consensus, any of the BIP8, BIP9, or Speedy Trial activation options could be used. If there is some controversy or a divided community, as was the case with SegWit, then activation might require a User Activated Soft Fork (UASF)-style path [UAS17]. As there's currently no meaningful agreement on either the introduction of PQC in the form of quantum-resistant signatures or on migration mechanism, it remains to be seen which approaches will be used for either of these activities.

Stakeholder Preparation and Ecosystem Coordination

Beyond technical activation, successful migration requires extensive market preparation tailored to different stakeholder needs across the Bitcoin ecosystem. Individual users and investors will require education campaigns and user-friendly migration tools, while institutional holders and custodians need implementation roadmaps, compliance documentation, and audit frameworks to maintain regulatory standing during migration. Exchanges face unique challenges due to their transaction volumes and hot wallet requirements, perhaps necessitating early access to private transaction services, while miners and mining pools may require infrastructure changes to support such services. The cost and requirements to run a full node may increase due to larger transaction sizes or transactions that are more costly to verify, which will impact those that support the Bitcoin network by running a full node.

Coordination across these diverse stakeholders presents significant challenges given Bitcoin's decentralized nature, but several approaches could facilitate an orderly transition. For example, technical working groups and the Bitcoin Core developer community would coordinate the development of migration standards and create reference implementations. For institutional players, regulatory engagement will be crucial, as migration transactions may have reporting and tax implications that need clarification before large-scale movement of funds occurs. The Bitcoin ecosystem would benefit from establishing clear communication channels and decision-making protocols well before quantum threats materialize, as last-

minute coordination would likely prove inadequate for managing a transition of this scale and complexity.

Decisions about the migration mechanism, activation approach, and timeline will emerge through the existing BIP processes and subsequent community deliberation. While technical considerations around migration mechanisms and activation methods are crucial, the chosen approach must also navigate the complex economic and governance implications for the entire ecosystem. Success will depend on both advanced preparation before quantum threats materialize and flexible response mechanisms if developments accelerate unexpectedly.

8. Path Forward

Bitcoin faces a significant but not imminent threat from the development of CRQCs, with experts projecting that CRQCs capable of breaking Bitcoin's elliptic curve cryptography could first emerge between 2030-2035. While this timeline doesn't necessitate rushed protocol changes, it does provide a critical window for thoughtful preparation. The Bitcoin community should accelerate research, development, and consensus building around quantum-resistant solutions, recognizing the substantial technical challenges involved and the complexity of Bitcoin's governance model.

Taking all currently available information and considerations into account, we propose a dual-track strategy for action that emphasizes prudent risk management over reactive crisis response. The dual-track approach is intended to recognize that although CRQCs are estimated to first appear in the next decade, there is always the possibility that they could appear earlier. As such, the Bitcoin community should begin a long-term effort to allow for a comprehensive exploration of the problem space, but should, in parallel, prepare more minimal solutions to act sooner, if necessary.

Short-Term Contingency Measures

It would be prudent to establish a minimum viable quantum-resistance option that could be implemented within a few short years and would be available for use either by those that wish to act early, or so that Bitcoin has at least some form of quantum resistance to fall back on while long-term approaches are still being investigated and developed. The priority is for practical, contingency protective measures that can be used if necessary, even if these measures are not optimized for long-term efficiency or are not suitable for all use cases. The solutions adopted as part of this endeavor will, in all likelihood, be superseded by more refined solutions as they are borne from the long-term comprehensive effort.

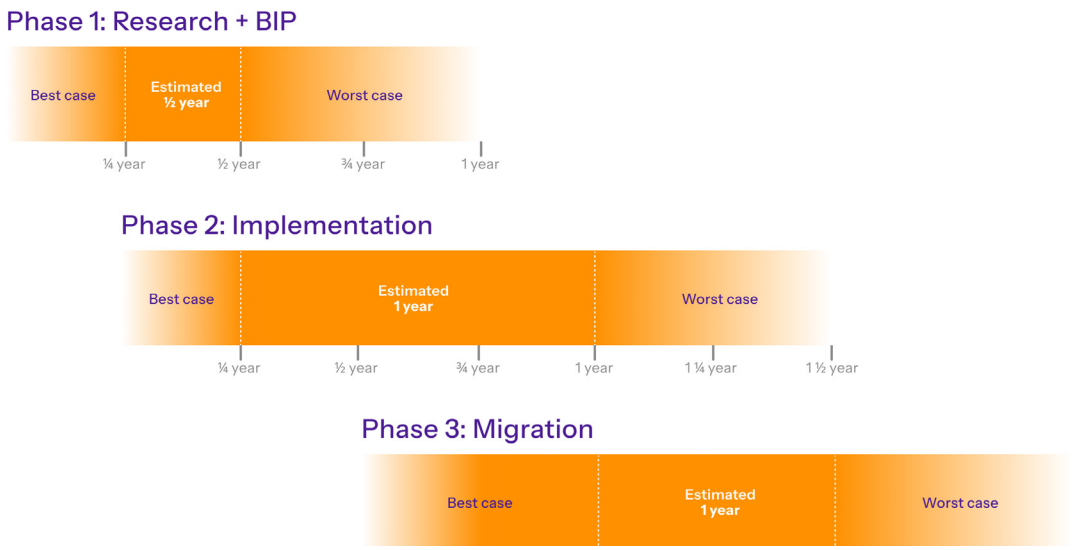


Figure 2. Timeline of estimate to establish short-term contingency measures.

The short-term contingency timeline visualization indicates that it would take approximately ~2 years for the estimate: initial research and BIP specification requiring 3 to 6 months, implementation between 3 and 12 months, and migration around 6 to 12 (as informed by UTXO Migration).

A shorter process, perhaps as short as ~1 year in total, can be expected if the community believes CRQCs are just around the corner. Achieving this would require immense coordination among Bitcoin Core developers and indeed the wider Bitcoin technical community. Also critical to success would be early engagement with institutional stakeholders who control large Bitcoin holdings with exposed public keys, given that they are the most at risk from a potential quantum attack.

Admittedly, there is little historical basis upon which this contingency timeline is based, as most significant protocol changes in Bitcoin have followed much longer development cycles (detailed in Long-Term Comprehensive Path). The Bitcoin community has, however, demonstrated capacity for rapid response to critical, albeit easily addressable vulnerabilities such as the 2018 inflation bug (CVE-2018-17144), which was resolved within days [BO19]. With the quantum computing threat representing a fundamentally different challenge to both upgrades that are without external forcing factors, like SegWit and Taproot, as well as critical yet simply resolved vulnerabilities like CVE-2018-17144, it seems that the indicative estimate of ~2 years for the completion of the full spectrum of activities on this contingency measures timeline is reasonable.

Long-Term Comprehensive Path

In parallel with the short-term contingency solution, a more thorough research and development effort is necessary to determine Bitcoin's optimal long-term quantum-resistant future. The research agenda must address several interconnected challenges that a post-quantum world presents.

First, post-quantum keys and signatures; most of the current options are significantly larger than ECC keys and signatures currently in use, potentially reducing Bitcoin's already limited transaction throughput. This may necessitate research into novel signature compression and aggregation techniques alongside the associated quantum-resistant signature algorithms. Second, migration mechanics; how should quantum-vulnerable funds be treated, and the practical considerations of moving tens of millions of UTXOs to quantum-resistant scripts.

Although Bitcoin mining will be impacted if quantum mining becomes feasible, we believe this to be significantly further into Bitcoin's future than the introduction of PQC and UTXO migration. As such, any further adaptation to Bitcoin required as a result of the impact of quantum mining is left as a future consideration.

To estimate how long a long-term comprehensive path may take, we examine the timelines of the two most recent and perhaps significant soft forks in Bitcoin: SegWit in 2017 and Taproot in 2021. SegWit (BIP 141) resolved the transaction malleability issue, which the community was aware of as early as 2011[20]. Experimentation on SegWit ideas started sometime in

20 But which gained widespread attention in early 2014 in playing a central role in the issues that led

early 2015 when Blockstream engineers prototyped the feature in the company's sidechain Elements, with development completed in Bitcoin Core by October 2016, a period of about 18 months [Van17]. After activating on the network in August 2017, its use in transactions has steadily grown, but it took about 6 years for 90% of transactions to consistently involve a SegWit spend, which could be seen as a measure of migration[21] [MO25a]. Thus, from conception to widespread adoption, the complete SegWit timeline stretched across ~8.5 years, beginning in early 2015 and achieving broad adoption by late 2023.

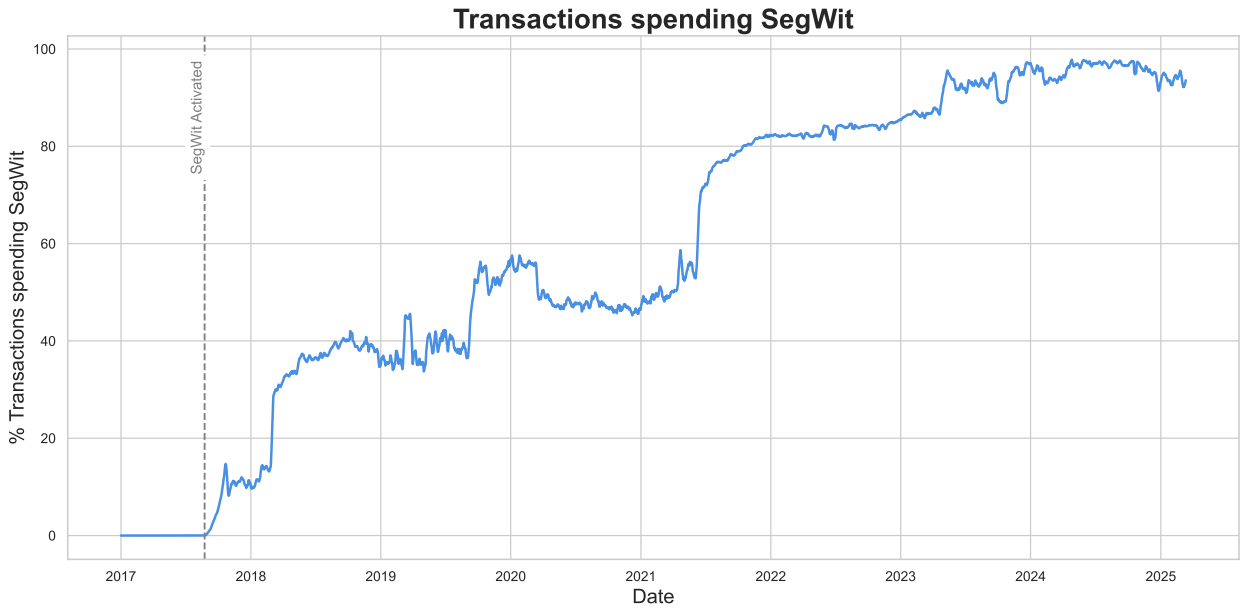


Figure 3. SegWit spending transactions, adapted from [MO25a].

to the downfall of Mt. Gox.

21 A transaction is considered to be SegWit spending when it spends at least one SegWit input [MO25a].

Taproot and Schorr (BIPs 340, 341 and 342) have similarly lengthy histories and timelines. The benefits of adopting Schnorr signatures in Bitcoin were discussed in various forms in the years 2012-2014 while Taproot was first discussed under the guise of Merkelized Abstract Syntax Trees (MAST) in the 2013-2014 period [Shi17]. The first BIP for MAST was proposed in early 2016 by Johnson Lau with BIP 114 [Lau16], but something closer to what became Taproot was proposed by Greg Maxwell 2 years later (January 2018) [Max18]. Another 2 years later (January 2020), BIPs 340, 341, and 342 were finalized, which is when the main development efforts in Bitcoin Core began [Shi21]. The changes were activated on the Bitcoin network in November 2021. The percentage of transactions spending Taproot in mid-2025 is currently ranging between 30 and 40%[22]. The combined Taproot and Schnorr changes were thus in progress, from original conception (early 2014) to activation (late 2021), for ~7.5 years, and the adoption is still ongoing[23].

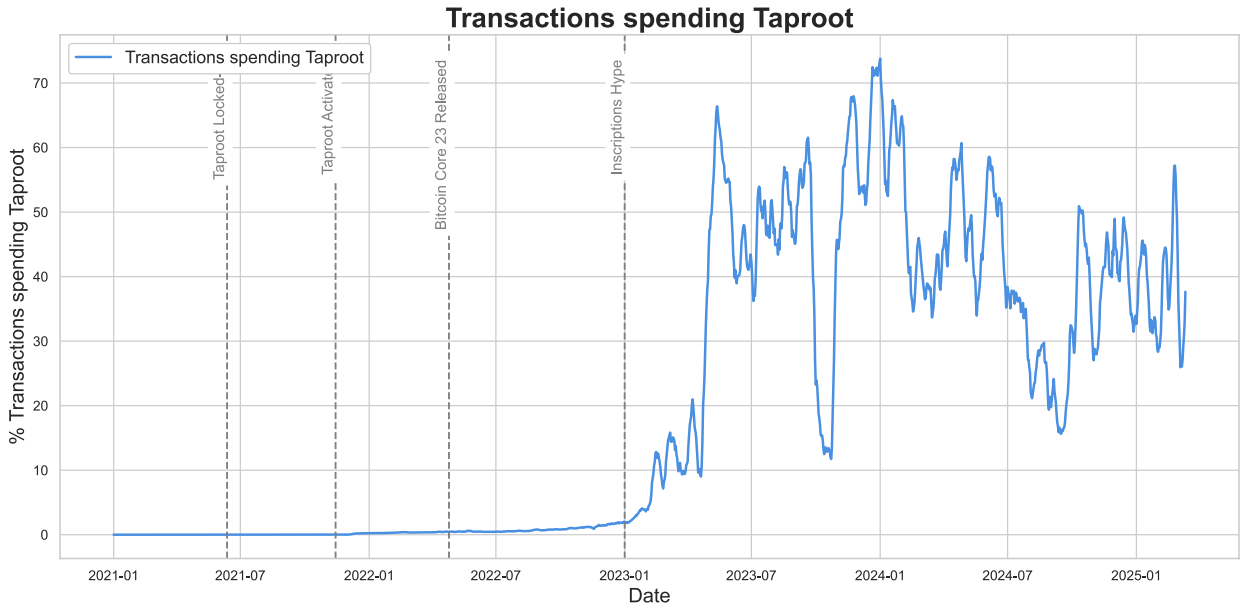


Figure 4. Taproot spending transactions, adapted from [MO25b].

Informed by the timelines for SegWit and Taproot, and considering broadly what needs to be achieved for Bitcoin to adapt to a post-quantum world, it is estimated that it would take approximately 7 years for a long-term effort to work through the stages of research and BIP, implementation, and then migration. Our timeline visualization illustrates how this range emerges from variable durations in each phase: research and BIP development (~2.5 years), implementation (~1.5 years), and migration (~ 3 years).

22 A transaction is considered to be Taproot spending when it spends at least one Taproot input [MO25b].

23 Unlike SegWit, which offered immediate fee savings for all during a period of network congestion, Taproot's adoption has been more gradual as its benefits are less pronounced for most users.

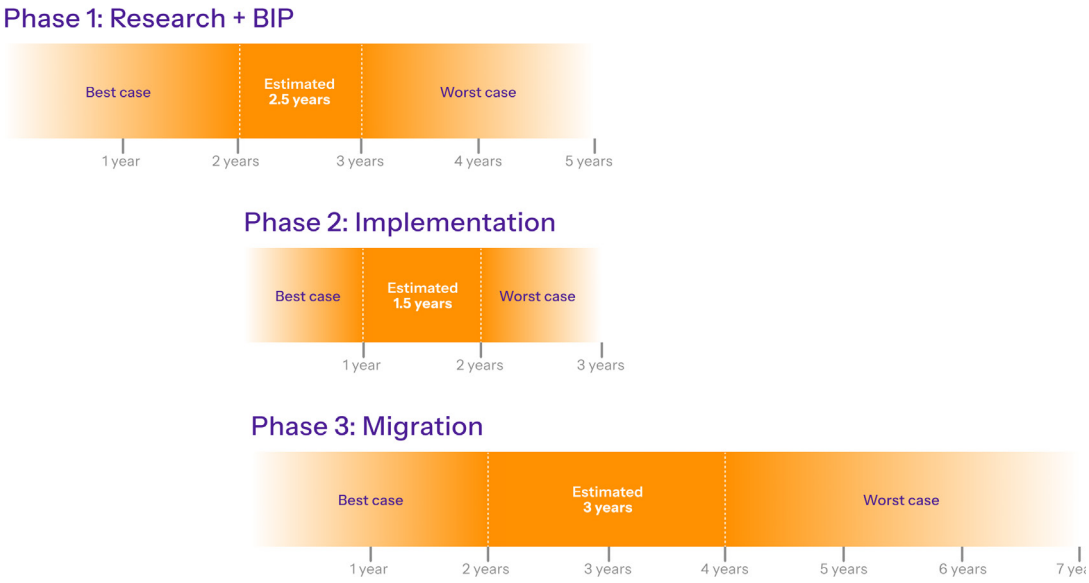


Figure 5. Timeline for Bitcoin's comprehensive quantum resistance path.

The wide variance reflects uncertainty in both technical challenges and building consensus amongst the community. In a best-case scenario where research proceeds quickly, implementation faces minimal complications, migration tools are widely adopted, and migration continues apace, the entire process might complete within 5 years. However, under the worst-case scenario, across all phases, the timeline could extend to 15 years. It should be emphasized that these best and worst-case scenarios are based on estimation rather than definitive evidence.

Projecting Forward

From the current state of quantum-resistant signature proposals, and ongoing community deliberation around migration strategies and technical implementations, projecting forward reveals several key transition points that may define Bitcoin's quantum-resistant future. The first key transition point is reached once quantum-resistant signature schemes are activated - this would permit the movement of quantum-vulnerable funds to permanent protection, such that funds would no longer be vulnerable in scenarios of address reuse or to short-range attacks. At that point, those that want to use the protection of quantum-resistant signature schemes can do so if they wish (noting that there may be significant cost to do so given the required resources as described in UTXO Migration), meaning funds that are permanently exposed to quantum attack (those that cannot be moved by their owners to more quantum-resistant script types) remain so.

The next transition point would be the implementation of the selected migration mechanism, which directly correlates with the community's deliberation on the burn vs. steal dilemma. Other than doing nothing, which would imply uninhibited quantum theft of remaining quantum-vulnerable funds, the various Migration Mechanisms propose consensus changes to establish protocol rules governing how unmigrated quantum-vulnerable funds can be accessed. Whether something like QRAMP's deadline-based approach, CDR's time-locked

commitment system, or the Hourglass strategy's rate-limiting mechanism, this transition point represents the concrete technical expression of Bitcoin's philosophical response to the quantum threat. Post this transition point, depending on both how quantum and classical computing capabilities evolve, it may be that further adaptation of Bitcoin is required to address the implications of quantum mining once they are truly known.

9. Conclusion

Recent announcements of quantum computing advances have brought new attention to Bitcoin's preparations for a post-quantum world. This report has examined how quantum computing intersects with Bitcoin's cryptographic foundations, the specific threats posed by cryptographically relevant quantum computers (CRQCs), and the potential solutions to maintain Bitcoin's security in a post-quantum environment. Our analysis covers the full spectrum of considerations, from Bitcoin's ECC-based transaction signature vulnerabilities and the threat of quantum mining, to technical proposals to introduce PQC and migrate quantum-vulnerable funds. We highlight the key philosophical challenge of whether vulnerable coins should be rendered unspendable ("burn") or allowed to remain retrievable by quantum attackers ("steal"). The report concludes with a proposed strategy and timelines for Bitcoin's successful transition to quantum resistance, designed to accommodate both current projections and the possibility of a significantly accelerated quantum breakthrough. The following is a summary of our findings, outlining the key considerations for this transition.

I. CRQC Timeline Assessment

Experts believe that CRQCs capable of breaking Bitcoin's ECC foundations could first emerge between 2030-2035, aligning with government directives to deprecate vulnerable cryptography by 2030 and disallow it by 2035. This projected timeline provides a crucial window for preparation, given the unpredictable nature of technological breakthroughs, it is essential to account for both the expected trajectory and the possibility of a significantly accelerated timeline.

II. Scope of Vulnerable Funds

Approximately 20-50% of all Bitcoin in circulation (4-10 million BTC) is potentially vulnerable to CRQC attacks. Long-range attacks target inherently vulnerable script types (P2PK, P2MS, P2TR) and addresses with previously exposed public keys (via address reuse), allowing attackers unbounded time to derive private keys from public information already available on the blockchain. Short-range attacks, which affect all Bitcoin script types, exploit the vulnerability window between transaction broadcast and confirmation (or shortly thereafter) when public keys are temporarily exposed, requiring attackers to act within a timeframe of minutes to hours.

Address re-use by exchanges and institutions has created a concentration of vulnerable coins in a small number of addresses - high-value targets that would likely be prioritized by quantum attackers. These holdings, however, represent a manageable quantum vulnerability, as owners retain the ability to transfer these funds to quantum-resistant script types when necessary, or can cease the practice of address reuse. This is in contrast to Satoshi-era and inaccessible quantum-vulnerable coins, which are permanently exposed to quantum attack as they cannot be moved by their owners to quantum-resistant script types.

III. Immediate Protective Measures

High-value Bitcoin holdings represent the most attractive targets for quantum attackers, particularly those of exchanges and institutions where address reuse practices have exposed public keys. While this creates a concentration of easily identifiable, valuable targets, the risk remains manageable through proactive measures. Since owners retain control of the private keys, vulnerable funds can be immediately migrated to somewhat quantum-resistant address types (P2PKH, P2SH, P2WPKH, or P2WSH). Simultaneously eliminating address reuse practices will prevent future exposure to long-range quantum attacks.

IV. Considerations for Bitcoin Mining

The quantum threat to Bitcoin mining via Grover's algorithm appears limited by physical and economic constraints. Quantum miners would face disadvantages including longer computation times, limited parallelization benefits, and substantially higher capital costs. Research indicates that quantum mining would remain economically impractical even with significant advances in quantum hardware, as the theoretical speedup from Grover's algorithm is insufficient to overcome the efficiency gap and lack of parallelization compared to specialized classical ASICs. This suggests mining security may prove significantly more resilient to quantum advances than transaction signature security.

If quantum mining does become viable, however, there's the potential for correlated fork events if quantum miners adopt aggressive mining strategies, which could lead to attackers with less than half of the network's hash rate being in a position to execute 51% attacks. And if quantum mining becomes the dominant means of mining on the network, the quantum superlinearity problem could drive extreme centralization, concentrating mining power among just a few operators.

V. Burn vs. Steal Dilemma

Perhaps the most significant challenge is not technical but philosophical: whether to "burn" vulnerable coins or leave them susceptible to being "stolen" by entities with CRQCs. This decision touches on Bitcoin's fundamental principles regarding property rights, censorship resistance, and immutability. The economic impact of either choice is substantial, with the potential for significant wealth redistribution or effective supply reduction. This is a polarizing issue, with strong opinions held by many on each side of the argument.

VI. Migration Pathways

The Bitcoin ecosystem's transition to quantum-resistant scripts faces significant technical and coordination challenges. Proposed migration mechanisms include the conservative commit-delay-reveal protocol that allows users to securely move their funds from non-quantum-resistant outputs to those adhering to a quantum-resistant signature scheme, the more assertive QRAMP protocol that would enforce migration deadlines after which vulnerable UTXOs become unspendable, and the hourglass strategy, which rate-limits vulnerable UTXO spending.

Successful migration necessitates unprecedented collective action by all ecosystem

participants - individual users, institutions, exchanges, and miners - with extensive preparation including education campaigns, migration tools, and regulatory engagement and compliance. The complexity of this transition demands establishing a shared vision and clear communication channels well before quantum threats materialize, as even the best technical solution will fail without effective cooperation among Bitcoin's diverse stakeholders.

VII. Strategy for Action

We propose that Bitcoin's quantum resistance strategy for action adopts a dual-track approach: contingency measures delivering minimal but functional protection against CRQCs completed in ~2 years, and a comprehensive path allowing thorough exploration of the problem space and the development of a full-featured approach to take ~7 years. This dual-track strategy balances immediate security needs with rigorous research and development of optimal quantum-resistant solutions, ensuring Bitcoin can respond appropriately regardless of how CRQC capabilities evolve.

VIII. Ongoing Efforts & Future Directions

Several technical approaches have emerged to address the potential for a CRQC to derive private keys and forge signatures. Each approach is of varying maturity, and there's currently no consensus on which direction to take. All current approaches also propose using PQC schemes that have combined public key and signature sizes that are many times larger than the combined size of existing ECC-based public keys and signatures. Given the strong focus on post-quantum cryptography within the broader cryptographic community, continued advancements are likely over time, offering the potential for more refined solutions as the field progresses.

Several leading cryptographers and Bitcoin developers who have contributed significantly to Bitcoin have begun working on quantum readiness strategies, joined by a number of new and enthusiastic contributors. While there's a vast solution space to explore, and the path forward remains uncertain, the community's ongoing efforts as outlined in this report should inspire confidence that Bitcoin will adapt to the post-quantum landscape in time. These efforts aim not only to meet projected timelines, but also to ensure readiness in the event of a sudden and significant leap in quantum computing capabilities.

10. References

- **[Aar24]** S. Aaronson. Recent developments in quantum computing. ShtetI-Optimized - The Blog of Scott Aaronson. September 16, 2024. https://scottaaronson.blog/?p=8329.
- **[ABL+17]** D. Aggarwal, G. K. Brennen, T. Lee, M. Santha, M. Tomamichel. Quantum attacks on Bitcoin, and how to protect against them. arXiv:1710.10377 [quant-ph]. October 28, 2017. https://arxiv.org/abs/1710.10377.
- **[ADM+16]** M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent, J. Schanck. Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3. Cryptology ePrint Archive, Paper 2016/992. October 17, 2016. https://eprint.iacr.org/2016/992.
- **[AIS25]** National Institute of Advanced Industrial Science and Technology (AIST). AIST and Intel Strengthen Collaboration for the Industrialization of Silicon Quantum Computers through MOU Signing. AIST News. February 6, 2025. https://www.aist.go.jp/aist_e/news/topics/au20250206_en.thml.
- **[And11]** G. Andresen. M-of-N Standard Transactions. Bitcoin Improvement Proposal (BIP) 11. October 18, 2011. https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki.
- **[ASE24]** Apple Security Engineering and Architecture. iMessage with PQ3: The new state of the art in quantum-secure messaging at scale. Apple Security Research Blog. February 21, 2024. https://security.apple.com/blog/imessage-pq3/.
- **[Bac18]** A. Back. Tweet about Johnson Lau's two-stage commitment proposal for post-quantum signatures. Twitter/X. January 2, 2018. https://x.com/adam3us/status/947900422697742337.
- **[Bal25]** P. Ball. Experts weigh in on Microsoft's topological qubit claim. Physics World. February 25, 2025. https://physicsworld.com/a/experts-weigh-in-on-microsofts-topological-qubit-claim/.
- **[BBH]** I. Barmes, B. Bosch, O. Haalstra. Quantum computers and the Bitcoin blockchain. Deloitte Risk Advisory. Undated. https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html.
- **[BDML]** Bitcoin Development Mailing List. https://groups.google.com/g/bitcoindev.
- **[Bea24a]** H. Beast. BIP-360: QuBit - Pay to Quantum Resistant Hash. Bitcoin Improvement Proposal (BIP) Pull Request 1670. September 2024. https://github.com/bitcoin/bips/pull/1670.
- **[Bea24b]** H. Beast. Proposing a P2QRH BIP towards a quantum resistant soft fork. Bitcoin Development Mailing List. June 10, 2024. https://groups.google.com/g/bitcoindev/c/Aee8xKuIC2s/m/cu6xej1mBQAJ.
- **[Bea25a]** H. Beast. Introducing Hourglass. Bitcoin Development Mailing List. April 30, 2025. https://groups.google.com/g/bitcoindev/c/zmg3U117aNc/m/IDCMs9j7EAAJ.
- **[Bea25b]** H. Beast (cryptoquick). LibBitcoinPQC. GitHub Repository. 2025. https://github.com/cryptoquick/libbitcoinpqc.

- **[BGN+22]** R. Benkoczi, D. Gaur, N. Nagy, M. Nagy, S. Hossain. Quantum Bitcoin Mining. Entropy (Basel), 24(3):323. February 24, 2022. https://doi.org/10.3390/e24030323.
- **[BIC25]** BitInfoCharts. Top 100 Richest Bitcoin Addresses and Bitcoin distribution. https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html.
- **[Bit25]** Bitmain. ANTMINER S21 XP Hyd. Bitmain Shop. https://shop.bitmain.com/product/detail?pid=00020250126221803633Izm03UGa06A1.
- **[BM14]** J. Bonneau, A. Miller. Fawkescoin: A Cryptocurrency Without Public-Key Cryptography. In: Christianson, B., Malcolm, J., Matyáš, V., Švenda, P., Stajano, F., Anderson, J. (eds) Security Protocols XXII. Security Protocols 2014. Lecture Notes in Computer Science, vol 8809. Springer. First online: 29 October, 2014. https://link.springer.com/chapter/10.1007/978-3-319-12400-1_35.
- **[BO19]** Bitcoin Optech. CVE-2018-17144. Bitcoin Optech. November 12, 2019. https://bitcoinops.org/en/topics/cve-2018-17144/.
- **[BP25]** F. Brandão, O. Painter. Amazon announces Ocelot quantum chip. Amazon Science Blog. February 27, 2025. https://www.amazon.science/blog/amazon-announces-ocelot-quantum-chip.
- **[BS24]** B. Bailey, O. Sattath. 51% Attack via Difficulty Increase with a Small Quantum Miner. arXiv:2403.08023 [quant-ph]. March 12, 2024. https://arxiv.org/abs/2403.08023.
- **[BSE18]** Bitcoin Stack Exchange Community. How did pay-to-pubkey hash come about? What is its history? Bitcoin Stack Exchange. April 6, 2018. https://bitcoin.stackexchange.com/questions/73563/how-did-pay-to-pubkey-hash-come-about-what-is-its-history.
- **[BTF]** BitcoinTalk Forum. https://bitcointalk.org.
- **[But13]** V. Buterin. Bitcoin Is Not Quantum Safe And How We Can Fix It. Bitcoin Magazine. July 31, 2013. https://bitcoinmagazine.com/technical/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150.
- **[But24]** V. Buterin. How to hard fork to save most users' funds in a quantum emergency. Ethereum Research Forum. March, 2024. https://ethresear.ch/t/how-to-hard-fork-to-save-most-users-funds-in-a-quantum-emergency/18901.
- **[Che25]** M. A. Cherney. Google says commercial quantum computing applications arriving within five years. Reuters. February 5, 2025. https://www.reuters.com/technology/google-says-commercial-quantum-computing-applications-arriving-within-five-years-2025-02-05/.
- **[CKR+20 (RG-1)]** F. Campos, T. Kohlstadt, S. Reith, M. Stöttinger. LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4. Cryptology ePrint Archive, Paper 2020/470. April 24, 2020. URL: https://eprint.iacr.org/2020/470.
- **[CLJ+16]** L. Chen, Y.-K. Liu, S. Jordan, D. Moody, R. Peralta, R. Perlner, D. Smith-Tone. Report on Post-Quantum Cryptography. National Institute of Standards and Technology Interagency Report 8105. April, 2016. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.
- **[CT10]** A. Chiesa, E. Tromer. Proof-Carrying Data and Hearsay Arguments from Signature Cards. ICS. Vol. 10. 2010. https://ic-people.epfl.ch/~achiesa/docs/CT10.pdf

- **[CMN23]** S. Choi, W. S. Moses, N. Thompson. The Quantum Tortoise and the Classical Hare: A simple framework for understanding which problems quantum computing will accelerate (and which it will not). arXiv:2310.15505 **[cs.DS]**. October 24, 2023. https://arxiv.org/abs/2310.15505
- **[Cor24]** M. Corallo. Trivial QC signatures with clean upgrade path. Bitcoin Development Mailing List. December 16, 2024. https://groups.google.com/g/bitcoindev/c/8O857bRSVV8/m/4cM-7pf4AgAJ.
- **[Cru25]** A. Cruz. Proposal for Quantum-Resistant Address Migration Protocol (QRAMP) BIP. Bitcoin Development Mailing List. February 12, 2025. https://groups.google.com/g/bitcoindev/c/8PM6iZCeDMc/m/PiGGU0hmAgAJ.
- **[CSE13]** Cryptography Stack Exchange Community. Quantum resistance of Lamport signatures. Cryptography Stack Exchange. June 29, 2013. https://crypto.stackexchange.com/questions/8931/quantum-resistance-of-lamport-signatures.
- **[DBF]** Delving Bitcoin Forum. https://delvingbitcoin.org.
- **[Dea25]** deadmanoz. Grover Parallelisation Notes. GitHub Repository. May, 2025. https://github.com/deadmanoz/pq-bitcoin/blob/main/notes/grover-parallelisation.md.
- **[Dra18]** J. Drake. Cryptographic canaries and backups. Ethereum Research. February, 2018. https://ethresear.ch/t/cryptographic-canaries-and-backups/1235.
- **[EOP25]** Executive Office of the President. Executive Order 14114: Strengthening and Promoting Innovation in the Nation's Cybersecurity. Federal Register, 2025-01470. January 16, 2025. https://public-inspection.federalregister.gov/2025-01470.pdf.
- **[Erh23]** Mark Erhardt (murchandamus). Statistics on current UTXO set. Dune Analytics Query 2962958. 2023. https://dune.com/queries/2962958/4909118.
- **[ETS15]** European Telecommunications Standards Institute. ETSI launches Quantum Safe Cryptography Specification Group. March 30, 2015. https://www.etsi.org/newsroom/news/947-2015-03-news-etsi-launches-quantum-safe-cryptography-specification-group
- **[ETS20]** European Telecommunications Standards Institute. ETSI Releases Migration Strategies and Recommendations for Quantum Safe Schemes. ETSI Newsroom. August 11, 2020. https://www.etsi.org/newsroom/press-releases/1805-2020-08-etsi-releases-migration-strategies-and-recommendations-for-quantum-safe-schemes.
- **[ETS21]** European Telecommunications Standards Institute. ETSI Releases Two Technical Reports to Support US NIST Standards for Post-Quantum Cryptography. ETSI Newsroom. October 6, 2021. https://www.etsi.org/newsroom/news/1981-2021-10-etsi-releases-two-technical-reports-to-support-us-nist-standards-for-post-quantum-cryptography.
- **[ETS25]** European Telecommunications Standards Institute. ETSI launches new standard for quantum safe hybrid key exchanges to secure future post-quantum encryption. ETSI Newsroom. March 25, 2025. https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption.
- **[FBS+23]** S. Farrell, F. Badii, B. Schneier, S. M. Bellovin. Reflections on Ten Years Past The Snowden Revelations. IETF Network Working Group. May 20, 2023. https://www.ietf.org/archive/id/draft-farrell-tenyearsafter-00.html.

- **[Gam24]** J. Gambetta. The hardware and software for the era of quantum utility is here. IBM Quantum Blog. December 4, 2024. https://www.ibm.com/quantum/blog/quantum-roadmap-2033.
- **[Gee23]** D. Geer. NIST post-quantum cryptography candidate cracked. Communications of the ACM. January 24, 2023. https://cacm.acm.org/news/nist-post-quantum-cryptography-candidate-cracked/.
- **[Gro96]** L. K. Grover. A fast quantum mechanical algorithm for database search. arXiv:9605043 [quant-ph]. May 29, 1996. https://arxiv.org/abs/quant-ph/9605043.
- **[GSM25]** GSMA. Post-Quantum Government Initiatives by Country and Region. GSMA Newsroom. March, 2025. https://www.gsma.com/newsroom/post-quantum-government-initiatives-by-country-and-region/.
- **[Hei25]** E. Heilman. Post Quantum Signatures and Scaling Bitcoin. Bitcoin Development Mailing List. April 5, 2025. https://groups.google.com/g/bitcoindev/c/wKizvPUfO7w/m/hG9cwpOABQAJ.
- **[Hoy18]** T. Hoy. Draft: Bitcoin's Post-Quantum Transition. Medium. May 31, 2018. https://medium.com/@tristanhoy/draft-bitcoins-post-quantum-transition-11271f430c41.
- **[HS23]** E. Heilman, A. Sabouri. OP_CAT in Tapscript. Bitcoin Improvement Proposal (BIP) 347. December 11, 2023. https://github.com/bitcoin/bips/blob/master/bip-0347.mediawiki.
- **[IBM24]** IBM Quantum. IBM Quantum Development and Innovation Roadmap. 2024. https://ibm.com/quantum/assets/IBM_Quantum_Developmen_&_Innovation_Roadmap_Explainer_2024-Update.pdf.
- **[ICC25]** Institute of Commercial Cryptography Standards, China. Announcement on Launching the Next-generation Commercial Cryptographic Algorithms Program (NGCC). February 5, 2025. https://niccs.org.cn/en/.
- **[JAC+22]** D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Hutchinson, A. Jalali, K. Karabina, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, D. Urbanik. SIKE: Supersingular Isogeny Key Encapsulation. NIST Post-Quantum Cryptography Standardization Process. September 15, 2022. https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/SIKE-spec.pdf.
- **[Jah25]** F. Jahr. Cross-Input Signature Aggregation (CISA) Research Report. Human Rights Foundation. March 21, 2025. https://hrf.org/latest/cisa-research-paper/.
- **[JL213]** jl2012. The use of Guy Fawkes Signature in case of ECDSA zero-day exploits. BitcoinTalk Forum. October 29, 2013. https://bitcointalk.org/index.php?topic=320634.0.
- **[Kre23]** E. Kret. Quantum Resistance and the Signal Protocol. Signal Blog. September 19, 2023. https://signal.org/blog/pqxdh/.
- **[Lau16]** J. Lau. BIP 114: Merkelized Abstract Syntax Tree. Bitcoin Improvement Proposal (BIP) 114. April 2, 2016. https://github.com/bitcoin/bips/blob/master/bip-0114.mediawiki.
- **[Lil25]** J. Lilic. Against Quantum BTC Confiscations: The 100 Year Hourglass Solution. Twitter/X. March 19, 2025. https://x.com/LilicJohn/status/1902076187821928873.

- **[Lin24]** R. Linus. OP_CAT Fallacies. GitHub Gist. August 22, 2024. https://gist.github.com/RobinLinus/fdee133af13948b0e617f9ef4f8b8752.
- **[Lit23]** D. Litinski. How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates. arXiv:2306.08585 [quant-ph]. June 14, 2023. https://arxiv.org/abs/2306.08585.
- **[Lop24]** J. Lopp. Safeguarding Satoshi's Stash. Presentation at Future of Bitcoin Conference. October 21, 2024. Youtube. https://www.youtube.com/watch?v=MTUzpR_mxAg.
- **[Lop25a]** J. Lopp. Against Allowing Quantum Recovery of Bitcoin. Cypherpunk Cogitations. March 16, 2025. https://blog.lopp.net/against-quantum-recovery-of-bitcoin/.
- **[Lop25b]** J. Lopp. Against Allowing Quantum Recovery of Bitcoin. Bitcoin Development Mailing List. March 16, 2025. https://groups.google.com/g/bitcoindev/c/uUK6py0Yjq0/m/NIRRiW-xAgAJ.
- **[LSN+25]** M. Liu, R. Shaydulin, P. Niroula, C. W. S. Lim, Y. Alexeev, M. Pistoia, S. Aaronson, S.-H. Hung, T. S. Humble, S. Keeney, N. Kumar, D. Lidar, M. L. Macneal, S. McCaskey, S. Merkel, K. N. Smith, E. R. Anschuetz, D. S. Schlegel. Certified randomness using a trapped-ion quantum processor. Nature, Vol. 640, pp. 343-348. March 26, 2025. https://www.nature.com/articles/s41586-025-08737-1.
- **[Max13a]** G. Maxwell. NSA and ECC. BitcoinTalk Forum. September 9, 2013. https://bitcointalk.org/index.php?topic=289795.msg3117127#msg3117127.
- **[Max13b]** G. Maxwell. Preparing for the Cryptopocalypse. Bitcoin Development Mailing List. August 4, 2013. https://gnusha.org/pi/bitcoindev/CAAS2fgTPFHGQVs8qUj+8NyRQ3Ym=ws=_+FuWWvyYra5r-PZsdQ@mail.gmail.com/.
- **[Max18]** G. Maxwell. Taproot: Privacy preserving switchable scripting. Bitcoin Development Mailing List Archive. January 23, 2018. https://gnusha.org/pi/bitcoindev/CAAS2fgTXg5kk6TyUM9dS=tf5N0_Z-GKVmzMLwTW1HxUgrqdo+Q@mail.gmail.com/.
- **[MDH24]** Marathon Digital Holdings. Slipstream: Direct Bitcoin Transaction Submission Service. February 2024. https://slipstream.mara.com.
- **[Mem25]** Mempool.space. Mempool.space - Mining. 2025. https://mempool.space/mining.
- **[MO25a]** Mainnet Observer by 0xB10C. Transactions Spending SegWit. Mainnet Observer. 2025. https://mainnet.observer/charts/transactions-spending-segwit/.
- **[MO25b]** Mainnet Observer by 0xB10C. Transactions Spending Taproot. Mainnet Observer. 2025. https://mainnet.observer/charts/transactions-spending-taproot/.
- **[MO25c]** Mainnet Observer by 0xB10C. P2PK Inputs and Outputs. Mainnet Observer. 2025. https://mainnet.observer/charts/inputs-and-outputs-p2pk/.
- **[MO25d]** Mainnet Observer by 0xB10C. UTXO set composition. Mainnet Observer. 2025. https://mainnet.observer/charts/utxoset-by-count/.
- **[MP24]** M. Mosca, M. Piani. Quantum Threat Timeline Report 2024. Global Risk Institute. December 6, 2024. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

- **[MPR+24]** D. Moody, R. Perlner, A. Regenscheid, A. Robinson, D. Cooper. Transition to Post-Quantum Cryptography Standards. NIST Internal or Interagency Report (NISTIR) 8547 (Draft), November 12, 2024. https://doi.org/10.6028/NIST.IR.8547.ipd.
- **[Nak10]** S. Nakamoto. Dealing with SHA-256 Collisions. BitcoinTalk Forum. June 14, 2010. https://bitcointalk.org/index.php?topic=191.msg1585#msg1585.
- **[Nak18]** S. Nakov. Practical Cryptography for Developers: Elliptic Curve Cryptography (ECC). GitHub Repository. 2018. https://github.com/nakov/practical-cryptography-for-developers-book/blob/master/asymmetric-key-ciphers/elliptic-curve-cryptography-ecc.md.
- **[Nay25]** C Nayak. Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits. Microsoft Azure Quantum Blog. February 19, 2025. https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/.
- **[NCS25]** National Cyber Security Centre. Timelines for migration to post-quantum cryptography. March 20, 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines.
- **[Nev24]** H. Neven. Meet Willow, our state-of-the-art quantum chip. Google Research Blog. December 9, 2024. https://blog.google/technology/research/google-willow-quantum-chip.
- **[NG21]** R. R. Nerem, D. R. Gaur. Conditions for Advantageous Quantum Bitcoin Mining. arXiv:2110.00878 [quant-ph]. October 2, 2021. https://arxiv.org/abs/2110.00878.
- **[Nic25]** J. Nick. Reply to P2QRH / BIP-360 Update. Bitcoin Development Mailing List. 2025. https://groups.google.com/g/bitcoindev/c/oQKezDOc4us/m/I6tmPaA2AgAJ.
- **[NIS24a]** National Institute of Standards and Technology. Module-Lattice-Based Key-Encapsulation Mechanism Standard. Federal Information Processing Standards Publication (FIPS) 203. August 13, 2024. https://csrc.nist.gov/pubs/fips/203/final.
- **[NIS24b]** National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. Federal Information Processing Standards Publication (FIPS) 204. August 13, 2024. https://csrc.nist.gov/pubs/fips/204/final.
- **[NIS24c]** National Institute of Standards and Technology. Stateless Hash-Based Digital Signature Standard. Federal Information Processing Standards Publication (FIPS) 205. August 13, 2024. https://csrc.nist.gov/pubs/fips/205/final.
- **[NIS24d]** National Institute of Standards and Technology. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. NIST News. August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.
- **[NIS25]** National Institute of Standards and Technology. NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption. NIST News. March 11, 2025. https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.
- **[NSA22]** National Security Agency. Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) FAQ. NSA/CSS. September 2022. https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

- **[OBr23]** D. O'Brien. Protecting Chrome Traffic with Hybrid Kyber KEM. Chromium Blog. August 10, 2023. https://blog.chromium.org/2023/08/protecting-chrome-traffic-with-hybrid.html.
- **[OMB22]** Office of Management and Budget. M-23-02 Memorandum on Migrating to Post-Quantum Cryptography. The White House. November 18, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.
- **[PE25]** Project Eleven Vulnerable Bitcoin Tracker. Project Eleven. Last updated January 17, 2025. https://www.projecteleven.com/btc-at-risk.
- **[PHN+24]** A. Poelstra, T. C. Harding, J. Nick, and rust-secp256k1 contributors. Rust language bindings for Bitcoin secp256k1 library. Rust Crate Documentation. 2024. https://docs.rs/secp256k1/latest/secp256k1/.
- **[PKM+24]** J. J. Pont, J. J. Kearney, J. Moyler, C. A. Perez-Delgado. Downtime Required for Bitcoin Quantum-Safety. arXiv:2410.16965 [quant-ph]. October 22, 2024. https://arxiv.org/abs/2410.16965.
- **[Poe24]** A. Poelstra. Script State From Lamport Signatures. Bitcoin Magazine. May 2, 2024. https://bitcoinmagazine.com/technical/script-state-from-lamport-signatures.
- **[PQC06]** PQCrypto Conference. PQCrypto - Post-Quantum Cryptography. Established 2006. https://pqcrypto.org/conferences.html.
- **[PQC15]** PQCrypto Consortium. Initial recommendations of long-term secure post-quantum systems. PQCrypto - Horizon 2020 ICT-645622. September 7, 2015. https://pqcrypto.eu.org/docs/initial-recommendations.pdf.
- **[PQS24]** PQShield. Post-Quantum Signatures Zoo: NIST round 2. PQShield Github Pages. October, 2024. https://pqshield.github.io/nist-sigs-zoo.
- **[PS22]** S. Park, N. Spooner. The Superlinearity Problem in Post-Quantum Blockchains. Cryptology ePrint Archive, Paper 2022/1423. October 20, 2022. https://eprint.iacr.org/2022/1423.
- **[Qua24]** Quantinuum. Quantinuum Launches Industry-First, Trapped-Ion 56-Qubit Quantum Computer, Breaking Key Benchmark Record. Quantinuum Press Releases. June 5, 2024. https://www.quantinuum.com/press-releases/quantinuum-launches-industry-first-trapped-ion-56-qubit-quantum-computer-that-challenges-the-worlds-best-supercomputers.
- **[QCS25]** Quantum Computing Stack Exchange Community. Why do people say that Grover's algorithm does not parallelize well? Quantum Computing Stack Exchange. November 12, 2022. https://quantumcomputing.stackexchange.com/questions/28968/why-do-people-say-that-grovers-algorithm-does-not-parallelize-well.
- **[Rin25]** Matteo Rini. Microsoft's Claim of a Topological Qubit Faces Tough Questions. Physics Magazine (APS), Vol. 18, 68. March 21, 2025. https://physics.aps.org/articles/v18/68.
- **[RR17]** J. J. Roberts, N. Rapp. Exclusive: Nearly 4 Million Bitcoins Lost Forever, New Study Says. Fortune via Web Archive. November 25, 2017. https://web.archive.org/web/20220628015523/https://fortune.com/2017/11/25/lost-bitcoins/.

- **[Ruf18]** T. Ruffing. Recovery of old UTXOs in a post-quantum world. Bitcoin Development Mailing List Archive. January 26, 2018. https://gnusha.org/pi/bitcoindev/1516972454.3107.67.camel@mmci.uni-saarland.de/.
- **[Sat18]** O. Sattath. On the insecurity of quantum Bitcoin mining. arXiv:1804.08118 [quant-ph]. April 22, 2018. https://arxiv.org/abs/1804.08118.
- **[SDS+24]** E. Strohmaier, J. Dongarra, H. Simon, H. Meuer. TOP500 List - November 2024 (64th Edition). TOP500.org. November 19, 2024. https://www.top500.org/lists/top500/2024/11/.
- **[Shi21]** Shinobi. Taproot Is Coming To Bitcoin: How It Works, Its History And Implications. Bitcoin Magazine. November 11, 2021. https://bitcoinmagazine.com/technical/bitcoin-taproot-explainer.
- **[Sho95]** P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. arXiv:9508027 [quant-ph]. August 30, 1995 https://arxiv.org/abs/quant-ph/9508027.
- **[SIZ+18]** I. Stewart, D. Ilie, A. Zamyatin, S. Werner, M. F. Torshizi, W. J. Knottenbelt. Committing to Quantum Resistance: A Slow Defence for Bitcoin against a Fast Quantum Computing Attack. Cryptology ePrint Archive, Paper 2018/213. February 26, 2018. https://eprint.iacr.org/2018/213.
- **[Spa25]** M. Sparkes. China launches hunt for ways to protect data from quantum computers. New Scientist. February 17, 2025. https://www.newscientist.com/article/2467574-china-launches-hunt-for-ways-to-protect-data-from-quantum-computers/.
- **[SW23]** O. Sattath, S. Wyborski. Protecting Quantum Procrastinators with Signature Lifting: A Case Study in Cryptocurrencies. Cryptology ePrint Archive, Paper 2023/362. March 12, 2023. https://eprint.iacr.org/2023/362.
- **[UAS17]** UASF Working Group. User Activated Soft Fork (UASF). UASF.org. 2017. https://uasf.org.
- **[Van17]** A. Van Virdum. The Long Road To SegWit: How Bitcoin's Biggest Protocol Upgrade Became Reality. Saylor Academy. August 25, 2017. https://learn.saylor.org/mod/book/view.php?id=30784.
- **[Wal25]** G. Walker. Hash Function. Learn Me a Bitcoin. January 16, 2025. https://learnmeabitcoin.com/technical/cryptography/hash-function/.
- **[Wik13]** Wikipedia Contributors. Merkle Signature Scheme. Wikipedia. Page added January 15, 2013. https://en.wikipedia.org/wiki/Merkle_signature_scheme.
- **[WNT20]** P. Wuille, J. Nick, and A. Towns. Taproot: SegWit version 1 spending rules. Bitcoin Improvement Proposal (BIP) 341. January 19, 2020. https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki.
- **[WR22]** B. Westerbaan, C. D. Rubin. Defending against future threats: Cloudflare goes post-quantum. Cloudflare Blog. October 3, 2022. https://blog.cloudflare.com/post-quantum-for-all/.

- **[Wui12]** P. Wuille. Hierarchical Deterministic Wallets. Bitcoin Improvement Proposal (BIP) 32. February 11, 2012. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki.
- **[Wui19]** P. Wuille. Tweet about magnitude of quantum-vulnerable Bitcoin. Twitter via Web Archive. March 19, 2019. https://web.archive.org/web/20220531184542/https://twitter.com/pwuille/status/1108085284862713856.
- **[WV24]** B. Westerbaan, L. Valenta. A look at the latest post-quantum signature standardization candidates. Cloudflare Blog. November 7, 2024. https://blog.cloudflare.com/another-look-at-pq-signatures/.