Finance and Economics Discussion Series

Federal Reserve Board, Washington, D.C.
ISSN 1936-2854 (Print)
ISSN 2767-3898 (Online)

"Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks

Jillian Mascelli, Megan Rodden

2025-093

Please cite this paper as:
Mascelli, Jillian, and Megan Rodden (2025). ""Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," Finance and Economics Discussion Series 2025-093. Washington: Board of Governors of the Federal Reserve System, https://doi.org/10.17016/FEDS.2025.093.

"Harvest Now Decrypt Later": Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks

Jillian Mascelli
Federal Reserve Board

Megan Rodden[*]
Federal Reserve Bank of Chicago

September 2025

Abstract

This paper analyzes the risks posed by future-state quantum computers, specifically the "harvest now decrypt later" (HNDL) risk. We review foundational concepts of quantum computing to address the present and ongoing threat of HNDL to currently protected data. We use the Bitcoin network as an illustrative example to study the implications of HNDL for distributed ledger cryptocurrency networks that rely upon traditional cryptography. We posit that while cryptocurrency distributed ledger network maintainers could successfully deploy post-quantum cryptography (PQC) mitigations to protect the network's security and data integrity against a future-state quantum computer, data privacy of the network's previously recorded transactions remains vulnerable against a future-state quantum computer due to HNDL. The difficulty in protecting data privacy lies in the risk that a bad actor can obtain a distributed ledger replica, harvest the data, and in the fullness of time reveal previously obfuscated and confidential data using a sufficiently powerful quantum computer. The authors highlight this gap in data privacy protection and note the shortage of mitigations for the data privacy risks associated with the HNDL threat within distributed ledger networks.

Keywords: payment networks, distributed ledger, technological innovation, quantum, peer-to-peer payments, data privacy, Bitcoin

[*] The authors would like to thank David Mills, Sonja Danburg, and Sarah Wright of the Federal Reserve Board; Troy Campbell and Kandice Alter of the Federal Reserve Bank of Chicago; and Dr. Dustin Moody of the National Institute of Standards and Technology (NIST) for their assistance with this paper. Disclaimer: the views expressed in this paper are solely those of the authors and should not be interpreted as reflecting the views of the Federal Reserve Board, the Federal Reserve Bank of Chicago, or the Federal Reserve System.

1 Introduction

Over the next two decades, commercially available quantum computers may be capable of operating more quickly and nimbly than legacy high compute alternatives. As private- and public-sector institutions invest in quantum computing technologies and error-correct computations (Swayne, 2025; Swayne, 2024), the promised computational power of quantum computers could become available commercially and to both good and bad actors. Increasingly fault tolerant and stable quantum computers will threaten existing public-key cryptography and may prompt legacy system maintainers to update their traditional cryptography to post-quantum cryptography (PQC) in response. [1] While this paradigm shift may present future operational and security risks, we highlight a present, active, and in some circumstances unavoidable data privacy risk posed by future-state quantum computers. This risk could be exploited through the actions known as "harvest now decrypt later" or HNDL.

In addition to the threats to centralized computer networks, sufficiently powerful and commercially available quantum computers operating within decentralized networks could pose a heightened risk to the data privacy of such networks operating with distributed ledgers or databases. Data privacy protections provided by traditional cryptographic methods in a decentralized, distributed ledger network may not sufficiently protect against a bad actor who independently stores a replica of the ledger with traditional cryptography ("harvesting") and the intent to break such cryptographic protection with a sufficiently powerful quantum computer and within a timeframe that such data is still deemed critical to protect from public view.

In this note, we will explore "harvest now decrypt later" (HNDL) as a present-day risk posed by future-state quantum computers to legacy computer networks. We focus on HNDL's current risks to decentralized distributed ledger networks, as explained in the following section, given their clear vulnerably to harvesting. We hypothesize that proposed solutions to protect the security and integrity of decentralized distributed ledgers against quantum computers, including network-wide encryption upgrades, do not fully mitigate the data privacy risks of future-state quantum computers. We further theorize that the HNDL risk's data privacy implications may not have any complete solution but instead pose a current and ongoing privacy risk to data originally encrypted with traditional public-key cryptography and intended to be permanently private.[2]

2 Assessment Approach

"Everyone knows that quantum mechanics is strange," Stanford professor Leonard Susskind observes at the outset of *Quantum Mechanics*, "but I suspect very few people could tell you

[1] The National Institute for Standards and Technology (NIST) refers interchangeably to "post-quantum encryption algorithms" and "post-quantum cryptography" as encryption methods capable of withstanding an attack by a quantum computer. In this paper, we refer generally to this concept as PQC, in keeping with NIST's standardized language (NIST, 2025c).

[2] While the standard lexicon of encryption might refer to such systems as "modern cryptography," as investigated in Katz and Lindell's *Modern Cryptography* (2014), this term seemed easy to confuse within the text of this paper. Throughout the paper, we refer to commonly used, non-quantum cryptography as "traditional" cryptography. As detailed in further sections, we consider traditional cryptographic methods to include public key cryptography.

exactly in what way." We authors are payment policy and technology researchers by background and interested in quantum computing as it relates to payment systems. We recognize that the depth and breadth of the term "quantum" is vast. Assessing the full scope of quantum computing threats would be a lengthy endeavor and outside the intent of this note. We have instead limited the scope of our analysis to a topic of research that is both payments-focused and applicable to the operations of payment systems, albeit distributed cryptocurrency systems. This note focuses on an assessment of the quantum-enabled risk termed "harvest now decrypt later" (HNDL) and its implications for transaction data privacy, with a case study using the distributed and decentralized cryptocurrency network Bitcoin to illustrate the HNDL risk for this type of payment network.

Our approach to this scope-limited analysis is as follows. Section 3 reviews the foundations of quantum computing to assist the reader's understanding of this emerging field and of quantum computing's relevance to a world of financial services supported by traditional computer networking. Section 3 then discusses the time-based imperatives of quantum computing and why we sought to understand some of the risks of future-state quantum computing capabilities to today's payment networks through this paper. Section 4 presents a case study of Bitcoin to illustrate several of these perspectives, namely the current risks of future-state quantum computers for decentralized and distributed payment networks. Section 4's case study identifies the HNDL risk and assesses how a sufficiently powerful and commercially available quantum computer could actualize the HNDL risk.

We make several assumptions throughout our analysis. First, our discussion of the HNDL risk assumes that a commercially available and sufficiently powerful quantum computer will, in the fullness of time, be available for control by a bad actor. We acknowledge that this timeline is ill-defined and the definition of "sufficiently powerful" differs depending on the strength of the underlying traditional cryptographic tools.[3] Further, we presume that a sufficiently powerful quantum computer may become first available to nation states, large corporations, and academic institutions operating such computers with expertise rather than lone bad actors. Yet, we presume that a bad actor, such as a malicious consortium or even a rogue nation state, could also acquire the means and expertise to secure a sufficiently powerful quantum computer.

[3] A "sufficiently powerful" quantum computer would need to be capable of breaking the traditional public key cryptography tools in question. For the purposes of this paper, the authors are not equipped with sufficiently robust academic material to either cite or generate the specific physical qubits required to crack every cryptographic tool used within typical distributed ledger networks, including the Bitcoin network. However, the cybersecurity research community is well suited to develop such research. Further, the narrow purpose of this paper is to emphasize the existing risks, and lacking mitigations, to data privacy within distributed ledger networks vulnerable to HNDL.

3.0 Quantum Computing

Quantum computing leverages quantum mechanics, a theory in physics that describes the behavior of light and matter in the presence of an observer.[4] These operations occur at the subatomic level, which cannot be observed with the naked eye. A quantum computer uses quantum bits, referred to as *qubits*, as the fundamental unit of information. This differs from traditional or classical computers, which use *bits* to carry out calculations. Classical computing bits are binary, meaning the bits can be 0 or 1. Bits allow classical computers to solve problems in sequential order and are deterministic in output; either 0 or 1, either *yes* or *no*, either A or B. Quantum computers instead use qubits, which can be 0, 1, or both simultaneously. The phenomenon of simultaneously existing as 0 and 1 is achieved through the quantum principles of superposition and entanglement. Pragmatically, this would allow for a quantum computer to operate significantly faster than a classical computer.

Superposition is the theory that qubits can exist in multiple states at the same time; qubits can be in a state that is a combination of both 0 and 1 until it is measured (or until a qubit is observed), it can exist in multiple states at once. Further challenging our intuition, qubits can also become entangled, meaning they share a single quantum state; qubits become linked with one another, and changes to one qubit will affect the other qubits, no matter the distance separating them. Quantum computers, in theory, could leverage both superposition and entanglement to increase computational speed by performing multiple data-processing operations at once. In short, through qubits behaving in superposition and entanglement, quantum computers can solve certain calculations or problems faster than the current power of classical computers. The development of Dr. Peter Shor's algorithm in 1994 piqued broader interest in quantum computing within the financial industry. Shor's quantum algorithm shows that with enough qubits, a quantum computer can break some forms of encryption, specifically public-key cryptography.

There are two primary encryption methods: symmetric and asymmetric. Symmetric key cryptography uses one private key to encrypt and decrypt data at rest (Mascelli, 2023, p. 9). This type of encryption is assumed to be less vulnerable to quantum computers compared to asymmetric encryption because the key sizes can be increased for protection. Asymmetric encryption, also called public-key cryptography or asymmetric key pair cryptography, uses a pair of keys to encrypt and decrypt data at rest or in transit. Each key can block or unblock data from view (Mascelli, 2023, p. 9). Traditional asymmetric cryptography is more vulnerable to quantum computing attacks because of Shor's algorithm. For example, Rivest-Shamir-Adleman (RSA)-2048 encryption is an asymmetric encryption method with a high strength key of 2048 bits and is the current encryption standard for data sent over the internet, the accepted norm for most applications and ensures that messages sent online have not been altered (Okta, 2024). RSA generates a public key, N, which is a product of multiplying two large prime numbers (p and q) together (N=pq). While N is public, both p and q are private. Factoring out the integers of the

[4]Susskind and Friedman (2015) offer a comprehensive review of quantum mechanics. We repurpose several of their general quantum mechanics concepts here on our way to discussing the basics of quantum computing. For example, they refer to *spin* while we refer to *qubits*.

public and private key back into the original prime numbers is incredibly difficult. This difficulty is what makes RSA so effective, because classical computers either cannot factor or require decades to factor the integer. Qubits would theoretically allow a quantum computer to decrypt a private key in hours to minutes, depending on the achieved power. A classical computer would take thousands of years to factor out numbers that are longer than 2048 bits (Ivezic, 2025), but Shor's algorithm shows that a quantum computer could do similar activities in minutes (Gidney, 2025). Similarly, Elliptic Curve Cryptography (ECC), another common asymmetric encryption method widely used to secure blockchain networks, relies on the discrete log problem, a mathematical task classical computers cannot currently solve in a reasonable timeframe. However, Shor's algorithm solves it. Quantum computers' exponential scale-up computing power threatens to decrypt both common encryption methods through their ability to factor out large integers or reverse complicated mathematic operations quickly. Large-scale quantum computers would be able to break the public-key cryptosystems currently in use, threatening the security, confidentiality, and integrity of classified communication and data globally.

Both quantum computers and classical computers work through circuits and gates, the building blocks for computational operations. For classical computers, an electrical circuit runs along wires and encounters what are called logic gates. These logic gates either allow or block electricity moving along the wire (like a physical gate blocking or allowing someone through). Electricity that moves through a gate represents a '1' bit, while a blocked gate (blocked electricity) represents a '0' bit (NIST, 2022). If a classical computer is given a problem to solve, electricity will run over a series of wires, encountering logical gates that measure as 1 or 0, subsequently reaching the solution. Logic gates being 'open' or 'closed' tells the computer how to carry out a calculation, enabling our daily computers to solve a variety of tasks.

Quantum circuits and gates measure qubits to find results. Like classical bits, qubits must go through a mazelike system but instead encounter quantum logic gates. Typically, a qubit will pass through a series of quantum gates that will manipulate the qubits quantum state to "[guide] its behavior at each step of the computation" (Zitter, 2025). Quantum logic gates face increased complexity due to qubits being unstable; engineers must maintain qubits stability throughout all gates. To reach a solution (the final step), a measurement gate collapses the qubits' ability to exist in multiple states simultaneously (superposition) and falls into a definitively classical value of 0 or 1, which can be measured. Quantum circuits can be designed for a single qubit or for multiple qubits. The number of gates a qubit goes through typically must be limited due to the extreme vulnerability of a qubit collapsing. Measurements in quantum computing need to extract enough useful information from the "whole set of results from the computations done in superposition" to be measured with accuracy (NIST, 2022). Through circuits and gates, scientists can measure qubits in superposition and entanglement to solve complex problems that classical computers currently cannot solve.

Not all qubits are created equal, and a sufficiently powerful quantum computer will require stable, error-corrected qubits. Most quantum computers today have noisy and error-prone qubits called *physical qubits*, which result in unreliable outputs. Since these physical qubits do not produce guaranteed 'correct' answers, adding more physical qubits increases the probability

that an output is correct. As more physical qubits are added, they can become 'connected' or 'structured,' which results in decreased errors. These are *logical qubits,* or perfect qubits. Logical qubits are abstract representations of fault-tolerant, error-corrected qubits, which provide more statistical certainty that an output is correct. The basic idea is that by adding more and more physical qubits, logical qubits are created, and these logical qubits are more likely to yield the correct answer.

Quantum computers need a sufficient number of logical qubits that correct errors faster than they accumulate to yield reliable outputs, a technique called quantum error correction (QEC). Multiple factors make this difficult to achieve: the cold conditions required for hardware, the monetary investment required for testing environments, the instability of qubits existing in superposition and entanglement, and the overall theoretical nature of studying subatomic particles. There are differing predictions for when a quantum computer will achieve sufficient computational power to render current cryptography methods useless, called *Q-Day* by some in the industry. For the purposes of this paper, the authors use the term Q-Day to describe when a future quantum computer will achieve sufficient error corrected, fault tolerant qubits capable of breaking asymmetric encryption.[5] Ultimately, Q-day is a moving target, yet the quantum threat remains.

3.1 What is the "Quantum Threat"?

The quantum threat is the potential risk that data encrypted using today's common standards will be deciphered by a future large-scale quantum computer capable of breaking some forms of cryptography before users can migrate to PQC (Figure 1). If PQC is not adopted collectively before a fault-tolerant quantum computer is achieved, asymmetric encrypted data and digital signatures are at risk; this risk increases alongside advancements in quantum. For example, Google's experimental quantum computer performed in three minutes and 20 seconds a calculation that the researchers reported would have taken IBM's Summit, the fastest supercomputer, 10,000 years to complete (Murgia and Waters, 2019). IBM later offered a public restatement of Summit's capabilities, estimating that Summit would require 2.5 years to conduct the same calculation (Lerman and O'Brien, 2019). One study estimated that a quantum computer with fewer than a million noisy qubits could factor RSA-2048 encryption in less than a week (Gidney 2025). These same computations would take classical computers thousands of years to complete (Okta, 2024). Payment system passwords, financial records, transaction data, and other personal data may be vulnerable to such a sea change in computing power.

While these calculations are theoretical predictions based on a multitude of variables, such as qubit type, they illustrate both the notable advancements being made in the industry and highlight the difficulty of accurately assessing the capabilities of supercomputers in units of time within the industry. [6] Qubits are fundamentally fragile, and their unstable nature can create errors

[5] More likely, "Q-Day" will be not a single day but a period during which systems become increasingly vulnerable to quantum computers, with the level of vulnerability dependent on the strength of traditional cryptography and cryptographic technologies.

[6] The type and stability of a qubit determines if it is fault-tolerant and error free. The testing environment (i.e. hardware and software) for qubits varies, and each type has advantages and disadvantages (NIST, 2025b).

before an operation can be completed, making it difficult to predict calculation times. As many firms continue to make progress toward fault-tolerant quantum computers, migration to quantum safe encryption is becoming an increasing priority for governments, financial institutions and standard-setting organizations (such as NIST). Rather than pinpointing a date for Q-Day, it might prove more beneficial for firms to instead identify the needed timeline to plan, prepare, and budget for transition to PQC.

3.2 Post-Quantum Cryptography Timeline

Scholarship is advancing to help determine the order in which common traditional cryptographic standards may become vulnerable to a sufficiently powerful quantum computer. Consequently, organizations could prioritize which traditional cryptography algorithms and hashing functions need transitioning to a standardized PQC option without needing a discrete timeline that specifies a Q-Day date of vulnerability. It is generally true and somewhat intuitive that increasing the bits of an encryption modulus (say, transitioning from RSA-1024 to RSA-2048) will increase the required physical qubits and time for a quantum computer to successfully break a vulnerable encryption method. [7,8] However, moving to a higher bit encryption method does not guarantee protection. If a quantum computer is capable of breaking RSA-1024, for example, it may be able to break RSA-2048 in a matter of months (Moody, comment, 2025). Additionally, transitioning to a higher RSA bit encryption can be costly and time-intensive for an organization. Similarly, ECC-256, the cryptography which authenticates digital signatures and is used to secure some cryptocurrencies like Bitcoin and Ethereum, can also be solved by Shor's algorithm. While breaking a 256-bit ECC key involves mathematically complex operations, if a sufficiently powerful quantum computer is achieved, it is still subject to be broken. Shor's algorithm solves the discrete logarithm problem that underpins ECC's security. One experiment demonstrated an approach for a quantum computer to break ECC by reducing cost per key "by a factor of 300-700 depending on the operating regime" (Litinski, 2023). Given that asymmetric cryptography, like ECC, is vulnerable to quantum computers, NIST has released guidelines deprecating and disallowing them over the next five to ten years (see Moody et al., 2024, p. 12-14). While experts cannot predict an exact date for Q-Day, and doing so may be a red herring altogether, we authored this paper under the assumption that timely migration to PQC could be important. [9] For the purposes of this paper, we framed our study and analysis of computational power in terms of physical processing limits rather than projected processing time.

In the *2024 Quantum Threat Timeline Report* authored by Michele Mosca and Marco Piani, a survey of experts generally agreed that a quantum computer could achieve 100 logical qubits in the next 10 years through notable implementation options, and one in three cybersecurity experts forecast that Q-Day will happen before 2032 (Mosca and Piani, 2024). However, the timeline to break a particular non-PQC algorithm varies depending on the quantum computer's qubits and the non-PQC algorithm's strength. Even with specific values defined,

[7] RSA-2048, a high strength key of 2048 bits, is the current encryption standard for data sent over the Internet, the accepted norm for most applications and ensures that messages sent online have not been altered. See Okta 2024.
[8] See Gidney, Google, 2021, page 3
[9] See Gidney, Google, 2021, page 2, for the quoted text.

experts still disagree on when a quantum computer will be capable of breaking traditional cryptography. This unpredictability may limit the willingness of firms and consensus groups to take the quantum threat seriously and to collectively move models toward quantum-resistant cryptography.

The development and implementation of PQC has become of paramount importance for many within the financial services industry and beyond, especially given the uncertainty around Q-Day. One of the leaders in the U.S. for developing, testing, assessing, and codifying PQC standards is the National Institute of Standards and Technology (NIST), which has developed cybersecurity frameworks and standards around quantum computing.[10] NIST defines PQC, also called quantum-resistant cryptography, as the development of "cryptographic systems that are secure against both quantum and classical computers and can interoperate with existing communications protocols and networks" (NIST, 2025c). To usher the migration to PQC, NIST has finalized three cryptographic standards around post-quantum encryption and five finalized quantum resistant algorithms (NIST, 2024, 2025a). NIST has advocated for organizations to begin implementing PQC algorithms and standards as soon as possible, and the U.S. Government has directed all federal agencies to migrate to PQC by 2035.

We shifted our framing of the decryption risk from time estimation to prioritization of encryption options based on their overall potential vulnerability to a sufficiently powerful quantum computer. Our prioritization is a rough estimate, however, and continual/ongoing research is needed to maintain appropriate prioritization as quantum computing and cryptographic technology continue to develop and new capabilities on both sides of the problem set emerge. This prioritization framework may prove helpful for all organizations to transition away from potentially vulnerable encryption methodologies and toward standardized PQC encryption. Rather than racing to accomplish a transition within a specific time range based on a fuzzily calculated threat arrival date, organizations could migrate complex systems in pieces, first prioritizing transitioning network assets protected by the most vulnerable encryption methods. Such prioritization could also assist in planning for transition costs across a diverse encryption portfolio.

[10] Cryptographic recommended standards published by NIST are provided primarily for the standardization of U.S. government systems and are not regulatory requirements. However, privacy sector and academic organizations may follow NISTs guidance to ensure interoperability with U.S. government systems.

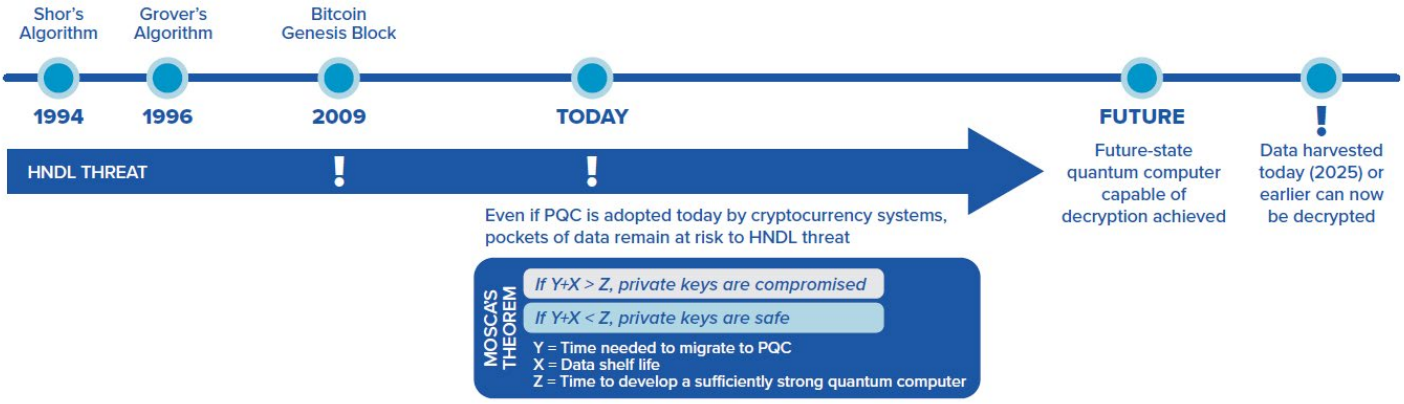

Figure 1. The HNDL threat began at the inception of Shor's algorithm in 1994 and remains ongoing. Data on the blockchain from 2009 onward is subject to the HNDL threat. For example, suppose a hypothetical cryptocurrency system has data on the blockchain with a shelf life of 10 years, and that data is harvested today (2025) by a bad actor. In two years (2027), the cryptocurrency system migrates to PQC, and in five years (2030), Q-Day happens. Even though the system migrated to PQC, the bad actor can decrypt the data in 2030 when a sufficient quantum computer is achieved. The data with a 10-year shelf life is not protected. Firms will need to consider the time it takes to migrate to PQC (Y) and the time data needs to remain protected (data shelf life) (X), and if that is *less* time than when a quantum computer is achieved (Z), firms will be able to protect their data. Thus, the relevance of Mosca's Theorem, which is discussed in detail in Section 4.3.

4.0 Case Study: "Harvest Now Decrypt Later" Data Privacy Threat for Bitcoin

As described at the outset of this paper and by Mascelli (2023), public-key cryptography secures blockchains, also called distributed ledgers. This approach has been integral to the success of distributed ledger networks' trustless operational models. However, as explored in the previous sections, public-key cryptography is particularly vulnerable to a sufficiently powerful future-state quantum computer. Further, in time a bad actor could obtain access to such a computer and look to disrupt the integrity, security, and data privacy of distributed ledger networks.

Some distributed ledger networks, particularly those that are public and permissionless, adhere to their own governance methods and requirements. There is no standard for the construction of a distributed ledger system at any level (ITU-T, 2023). Due to this, some distributed ledger networks may not or cannot support collective migration to a new version of a blockchain in support of a full-network PQC protection. Relatedly, permissionless distributed network systems are open to anyone to perform operations on the ledger or see transactions and trades. Yet, these same elements expose distributed ledger networks to adversaries (Scholten, et al., 2024), including bad actors who intentionally keep replica copies of the blockchain ledger for future exploitation by sufficiently powerful quantum computers. It is this paradigm that we analyze

further, using the distributed ledger network Bitcoin as an example of permissionless distributed ledger network's particular risks to data harvesting.

This case study analyzes the impact of PQC to a public, permissionless distributed ledger network like Bitcoin and concludes that the HNDL threat is (1) current and active within Bitcoin; (2) without significant data privacy mitigations for transactions completed before PQC is substantially deployed within the network; and (3) activated on an asynchronous timeline because of the varying strengths of the traditional cryptographic tools used within Bitcoin's decentralized networks. With sufficient technical know-how, a bad actor could join the Bitcoin network as a node operator, harvest a copy of the network's database (here, the blockchain ledger), independently store their ledger copy without PQC protection, and in the fullness of time pull their ledger replica into a quantum computing environment to crack the traditional cryptography, attack the protections of private keys, and reveal the blockchain ledger's data in plain text. The following sections discuss this process, and potential mitigations, in greater detail.

4.1 The Bitcoin Network

Bitcoin is a distributed ledger network with a roughly 15-year ledger history, a permissionless access structure, and diverse usage of encryption, hashing, and encoding schemes to provide a permissionless and decentralized peer-to-peer payment network while preventing ledger tampering. The Bitcoin network's resulting distributed ledger is public and permissionless, meaning any computer node (with sufficient free space, memory, internet connection, and electricity source) operator can join the network and receive a continuously updating replica of the Bitcoin blockchain. These elements make Bitcoin a helpful example of the type of distributed, permissionless, and long-running financial databases that might be particularly vulnerable to the HNDL threat to data privacy.

4.2 Traditional Cryptography usage in the Bitcoin Network

Cryptography is a critical tool enabling multiple functions for Bitcoin in furtherance of the network's goals for security, confidentiality, and immutability. These cryptographic tools are a part of an interconnected web of protection that includes encryption algorithms, hashing, key pairs, and encoding. Together, they ensure that bitcoin senders, bitcoin receivers, and service providers within the Bitcoin ecosystem can rely on some level of transaction security, pseudonymous confidentiality, and ledger accuracy.

When a "full node" operator first joins the Bitcoin network, they must conduct an initial block download to obtain and synchronize a local replica of the shared Bitcoin ledger, which amounts to downloading the entire Bitcoin blockchain, and download the Bitcoin Core operational software (Bitcoin Project, 2025). This initial node setup process is where a node operator first obtains a local replica of the full ledger and first encounters cryptographic tools within the Bitcoin network. This continuously updating replica ledger provides a node operator with an accurate history of previous bitcoin transactions, network updates, and data transfers (Bitcoin Project, 2025). Node operators use key-pairs and SHA-256 cryptographic function

hashes, partly provided by Bitcoin Core software maintainers, to complete the onboarding process.

Some Bitcoin users, however, lack the requisite computational power, upkeep time, or financial resources required to run a full Bitcoin node. Additional ways to interact directly with cryptography within the Bitcoin network include: downloading bitcoin wallet software onto your computer or mobile device to receive or buy Bitcoin; obtaining a physical hardware storage device with bitcoin storage software pre-loaded onto the device ("hardware wallet"), often a USB memory stick; and accepting bitcoins as a means of payment through a Bitcoin wallet provider or cryptocurrency payment processor.[11] Connecting directly to the Bitcoin network via a full node offers the most detailed view into the cryptographic tools used within the network. For the remainder of this section, we review the Bitcoin network's cryptographic tools from the vantage point of a full node operator rather than, say, a passive bitcoin holder or third-party service user. Figure 2 provides a high-level view of this process, including how a node operator first interacts with cryptography within the Bitcoin network (steps 2 and 3) and obtains a full replica of the ledger to store locally. Figure 3 visualizes the cryptographic tools and nesting processes to create a Bitcoin address. Badev and Chen (2014) also offer a helpful overview of how key pairs are used to create a Bitcoin address.

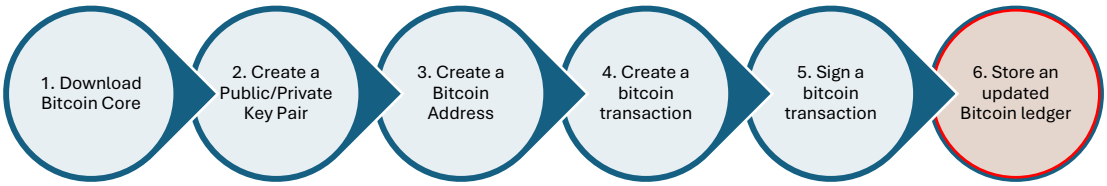

Figure 2: Illustrative order of obtaining a local replica of the Bitcoin ledger as a full node operator

Note: Step 6 in Figure 2 is the step that introduces the most vulnerability to the HNDL threat should a bad actor acquire a replica of the Bitcoin ledger, currently protected without post-quantum cryptography, and in time also acquire a sufficiently powerful quantum computer to break the traditional cryptography protecting the replica of the Bitcoin ledger.

To create a Bitcoin address, a user first generates a private key, which is akin to a password, and a public key using open-source key generation software. The public key and private key are cryptographically paired. The private key appears to the user as a long, random string of characters. The private key is meant to be kept secret by the user. Separately, the user is free to share their public key with others. The sharable public key, however, is a long mess of characters, easy to mistype and clunky to share. Bitcoin solves this by allowing users to apply an

[11] See Bitcoin Project (2025) and PayPal (2025) for additional resources on connecting directly or indirectly to the Bitcoin network. Exposure may also be intermediated by third-party service providers and node operators who are directly connected to the network.

encoding scheme to the public key. Encoding the key creates a short, user-friendly Bitcoin address shown as a more easily readable set of letters and numbers. An address is a unique string of alphanumeric characters, and multiple address formats are available depending on the user's preference and needs. Badev and Chen (2014) point out that possessing a Bitcoin address is tantamount to possessing the private key associated with the public key of that address. The user records their encoded Bitcoin address on the Bitcoin blockchain, and (trivializing additional technical setup steps) the user's Bitcoin address can receive and send bitcoins somewhat like a bank account receiving and sending funds from other bank accounts (Febrero-Bande et al., 2022).

Creating a Bitcoin address, summarized:

Step 1: Create private key and store it securely

Step 2: Apply Elliptic Curve Cryptography to the private key to create a long public key

Step 3: Apply a cryptographic hashing function (that is, SHA-256) to the public key

Step 4: Use an encoding scheme to shorten the resulting hash of the public key

Step 5: Store the resulting address, shown visually as a short string of characters

Bitcoin address creation has evolved over time, as have the cryptographic tools used to create and encode addresses. Yet, legacy Bitcoin address types commonly used in the early days of the Bitcoin network and modern address formats all use a public key and a combination of cryptographic tools to produce a resulting address (Choy, 2024). While different types of Bitcoin addresses result from varying combinations of tools with the public key, the address generation process employs the same three types of cryptographic tools: a cryptographic algorithm, cryptographic hash functions, and an encoding scheme (see figure 3). The relationships between the encryption algorithm, cryptographic hash functions, and encoding scheme are illustrated in the table below, derived from both the literature study provided by Febrero-Bande et al. (2022) and the Bitcoin address comparisons by Choy (2024). The diversity of Bitcoin address types allows users to select the address type that best suits their needs and security preferences. This diversity may imply that some legacy address types, and the transaction data associated with them, could become vulnerable to quantum computers sooner than other address types.[12]

[12] As an aside, technology maintainers and users may choose to prioritize transitioning their cryptographic tools to PQC standards in order of underlying cryptographic vulnerability in a tiered approach. For the illustrative graphic above, this may mean transitioning more vulnerable encryption algorithms to PQC standards first, then focusing on hash functions, then encoding schemes, if relevant to PQC needs.

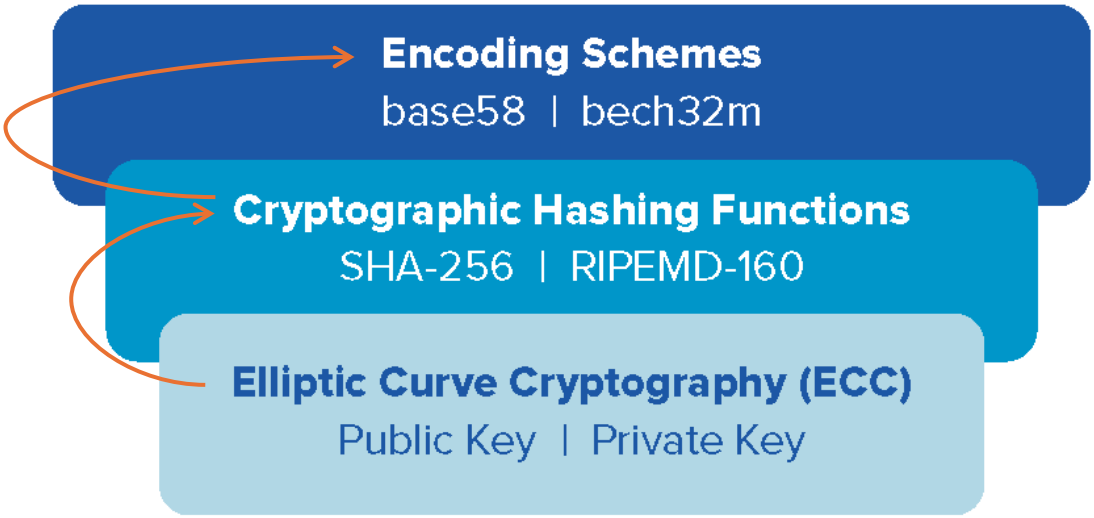

Figure 3: Depiction of the nested relationship between cryptographic algorithms, cryptographic hash functions, and encoding schemes used to create a Bitcoin address.

4.3 HNDL Risks for Bitcoin's Distributed Ledger Networks

For distributed, decentralized, and permissionless blockchain networks like Bitcoin, HNDL is a possible threat to the network's asymmetrically encrypted or cryptographically protected data at rest or in motion. Such data could be collected by a bad actor today and stored until a sufficiently powerful quantum computer breaks the traditional cryptography and unmasks the data into plain text. Notably, this issue is not limited to Bitcoin but is a current and known cybersecurity concern for a wide variety of encrypted data on computer systems around the world.

What are the risks?

Future state quantum computers present several general risks to the Bitcoin network. The most prominent of these risks may be exploiting Bitcoin's lag time to settle transactions given that a sufficiently powerful quantum computer could operate faster than Bitcoin can add a new block to its ledger, detangling Bitcoin's protections faster than the Bitcoin network can operate (Barmes et al.). This scenario might allow for a bad actor to tamper with the blockchain, threatening the data integrity of the distributed ledger. This race, though, is a forward-looking risk scenario and outside the narrow scope of our analysis. For our focus on the present data harvesting risk, we hold that HNDL poses two primary threats to the Bitcoin network: revealing confidential encrypted data (data privacy) and stealing funds.

HNDL threatens to expose private data associated with Bitcoin addresses, especially legacy addresses, which are used to prove ownership of funds and authorize outbound transfer of funds. This threat may reveal address-specific transaction data not already apparent from the blockchain's public nature. This threat may also facilitate further heuristic analysis of Bitcoin transactions not already discoverable through commercial blockchain investigative tools, especially allowing deeper analysis of early transactions with dormant legacy addresses. Further, data encoded in smart contract operations, digital signatures used to authorize transactions,

public keys associated with active wallets, long-term financial contracts recorded on the blockchain, and otherwise private communications on the network can all be stored today by a bad actor for later unmasking in the decade(s) to come.

We also sought to address the total value of bitcoins or addresses which might be vulnerable to theft by a quantum computer and most ripe for data harvesting. In our review of available literature, we did not identify conclusive, peer-reviewed calculations for the total value of bitcoins that would become vulnerable should a powerful quantum computer (or a cohort of quantum computer nodes) attempt to assume control of the Bitcoin network and its governance controls. As we came to better understand the HNDL risks for Bitcoin's unique web of cryptographic tools, we also identified the "total value" activity as less helpful than identifying remainder risks that could not be fully resolved with network-wide PQC mitigations. The calculation of vulnerable bitcoins and addresses may shift dramatically should any PQC mitigations be deployed to protect abandoned legacy addresses and earlier-mined bitcoins before a sufficiently powerful quantum computer is introduced into the network.

Yet, the act of quantifying the total amount of vulnerable bitcoin may assist these mitigation efforts by highlighting the areas of greatest vulnerability within the network to prioritize PQC mitigation strategies. While lacking scientific rigor, one informal piece of analysis from the Bitcoin community attempts to quantify the value of vulnerability within the Bitcoin network. We do not replicate that calculation here for the reasons just stated, but the author presents quantitative analysis suggesting that vulnerability is concentrated in legacy addresses and earlier-issued bitcoins protected with weaker traditional cryptography than, say, cryptographic methods a user might select if they were creating a Bitcoin address today. This assumption aligns with our findings. The same cryptographic weaknesses identified for earlier-minted bitcoins also applies to legacy dormant Bitcoin addresses which are locked or otherwise still contain some value of bitcoins protected only by traditional cryptography. Quantum-vulnerable Bitcoin address types may include earlier types of addresses, reused addresses, and Taproot addresses (cryptoquick, 2024). This may even include early Bitcoin address(es) associated with the network's founder(s), Satoshi Nakamoto.[13] While community analysis identifying the types of vulnerable addresses is untested, it follows logical sense. First, legacy addresses are based on weaker traditional cryptographic tools than more recent Bitcoin address types. Second, reused addresses offer a bad actor more historical data for harvesting, analysis, and later exploitation. Third, Taproot addresses were meant to be an improvement to the network, offering more privacy to end users. However, Taproot addresses, and their data privacy benefits, are still vulnerable to a quantum computer because they rely upon ECC, specifically Schnorr signatures (cryptoquick, 2024).

We find, then, the task of quantifying all quantum vulnerable bitcoins to be intellectually interesting but operationally something of a red herring, and so we turn our attention away from

[13] See Hunt, 2024. This assumes that Bitcoin community lore is correct in that Satoshi Nakamoto owned at least one of the early Bitcoin addresses which retain value but remain dormant. Early Bitcoin addresses relied upon ECDSA, which we detail elsewhere as quantum vulnerable.

theft toward the HNDL risk scenario for which we find no apparent mitigation, namely broken data privacy and plaintext data revealed for unfettered analysis.

What is the risk duration?

Data owners may not perceive their data as being presently stolen, harvested, or even at risk from a quantum computer. Yet, any Bitcoin data at risk to a sufficiently powerful quantum computer has been at risk since the network's creation.[14] This long-running risk is due to the discovery of Shor's Algorithm well before the creation of Bitcoin; the use of quantum-vulnerable cryptographic tools since the Genesis Block; and these tools being in use from the earliest iterations of Bitcoin addresses. For a full node operator, the length of the risk begins with the node operator's interactions with these tools, as laid out in the previous section, which likely coincides with their earliest interactions with the network and private key creation.

The "end date" of the HNDL risks is not as definite as the start date, and this end date may differ from node to node depending upon the network's longer-term PQC migration strategy. Evaluating the amount of time that data needs to remain secure, also called the shelf life of the data, may help determine how to evaluate the HNDL threat timeline for Bitcoin nodes. As described by Mosca's Theorem, the shelf life of data (X) plus the time required for an organization to implement PQC solutions (Y) must be greater than the time it will take for a sufficiently powerful quantum computer to be developed that can break existing encryption protocols (Z,) (X+Y > Z) (Figure 1). If X+Y>Z, then secret keys and private data are at risk and subject to an attack or HNDL. However, if X+Y<Z, then secret keys and data are in good shape if migration begins now. Determining these figures are largely dependent on the subjective nature of how long Bitcoin users would desire their cryptographically obfuscated data to remain private compared to the timeline for which the Bitcoin network migrates to fully or primarily PQC tools.

Migrating or updating cryptography methods is a complicated process and requires time. No matter if an organization waits for standardized PQC, it could take ten or more years for the algorithm to become fully integrated into information systems (NIST, 2025c). Further, even if Q-Day does not occur for two decades or longer, a distributed ledger network relying on a decentralized governance model may need years for planning, testing, adopting, and deploying PQC across the network to prepare for the eventuality. Such migrations may prove cumbersome, costly, and iterative. Complex cryptocurrency networks may benefit, then, from becoming be cryptographically agile, adopting "crypto agility" into the core of the governance model, as quantum computers continue to develop and advance in new ways. Rather than adopting a static suite of cryptographic tools and targeted a specific "Q-Day" for migration, network maintainers and node operators may find themselves continuously updating to and between quantum-resistant algorithms to match the pace of improvements in quantum computing. As such, the "end date" of the HNDL threat may itself be a multi-phased timeline, if not a moving target.

[14] See also documentation for BIS Project Leap (BIS, 2023, p. 7,10, 13).

4.4 HNDL Mitigations and Limitations

The same properties that might heighten Bitcoin's HNDL vulnerabilities may also provide opportunities for mitigation. For instance, not all Bitcoin data is subject to the HNDL data privacy risk, given that some data is intentionally public. Because the blockchain is decentralized and open in nature, any publicly visible transaction data, including payloads and pseudonymous identifiers, are notably not subject to the HNDL data privacy risk, as this information is already publicly accessible.

We observe that the Bitcoin community is already intensely considering multiple avenues toward PQC protection for the Bitcoin network.[15] These possible mitigations focus on the integrity of the blockchain, preventing or reversing theft, and ensuring the future crypto agility of the Bitcoin network.

The Bitcoin community could explore several mitigations for the threats presented in the previous section: theft of funds, tampering with the blockchain (data integrity), and revealing otherwise confidential data (data privacy). Momentarily, we will set aside data privacy mitigations and focus on maintaining trust in the blockchain and combatting theft. Mitigations for data integrity and theft include instituting a hard fork toward a PQC-only blockchain, adopting PQC standards across the larger Bitcoin ecosystem with a push towards crypto agility, requiring all addresses and third-party services to adhere to PQC standards, and/or encouraging heightened security hygiene practices.

The Bitcoin network could make available a new version of the blockchain that only uses post-quantum encryption like Vitalik's suggestion for Ethereum (Buterin, 2024). A hard fork toward a PQC-only blockchain might facilitate the restoration of stolen funds, however the Bitcoin developer community may be mixed on this approach and prefer a voluntary change. A voluntary change, such as a soft fork, would allow users to upgrade on a timeline that met their goals while respecting node operators' resourcing restrictions. A hard fork or soft fork would require backward compatibility to protect all historically harvested data. Yet even a backwards-compatible fork may leave open the HNDL data privacy vulnerability. Some users may choose not to migrate to PQC or the new fork at all. Users that remained on a non-PQC version of the blockchain could become increasingly vulnerable to security, financial, and data privacy risks of a future-state quantum computer. Instituting a hard fork with a quantum-resistant version of the blockchain might ensure that the network's time to mine a new block is quicker than a quantum computer can act to tamper with the block's data integrity, yet such an approach may be increasingly difficult to reinforce as quantum computers become more powerful. We believe the Bitcoin community to be knowledgeable about these risks, capable of weighing the costs and benefits of a forking to achieve crypto agility, coming to consensus on a long-term action plan, and continuously upgrading the network's cryptographic protections. The difficult question to answer is the extent of adoption by a diverse community of Bitcoin users, with highly varied goals and requirements, and the resulting PQC protections for the network. The Bitcoin

[15] These could include a mandatory hard fork alongside new PQC address types (Cruz, 2025). See also Buterin (2024) for an Ethereum hard fork proposal.

community is capable of rapid adoption and adaptation for the benefit of the network, yet forced migrations seem well outside the ethos of the community. As a further mitigation, then, the community may benefit from expert engagement on the security, integrity, and privacy advantages of PQC and crypto agility.

Adopting updated PQC-compliant cryptographic tools, specifically PQC address type(s) to replace legacy and Taproot addresses, is another possible mitigation and might not require a hard fork (cryptoquick, 2024). As discussed earlier in this paper, NIST has published several PQC standards that could facilitate this migration to new address types. However, if a user with a "PQC safe" address completes a transaction with an "unsafe" address, both may still be vulnerable to data harvesting and theft by a quantum computer. The network's governance structure could, then, require all wallets and third-party services to use PQC methods moving forward. Yet this, too, may be difficult to enforce given the highly decentralized nature of the Bitcoin network, the lack of a central enforcement authority, and the network's culture valuing choice over force.

Lastly, the network could mitigate theft risks posed by a quantum computer by improving security hygiene throughout the network. This could include not reusing Bitcoin addresses through multiple transactions, even those protected with PQC. Yet again, enforcing rather than encouraging such hygiene would be antithetical to the network's decentralized structure. Notably, each of these mitigations require security-through-force rather than security-through-adoption. This may present a cultural challenge for the Bitcoin community, which relies upon a decentralized governance structure.

However, even if the community collectively, willingly, and fully adopted each of these mitigations, one of the three key vulnerabilities would remain without a full solution: data privacy. First, transitioning to only PQC address types, for example, does not retroactively protect a Bitcoin user's previous transactions with less–quantum resistant address types. A user could transfer their bitcoin funds from a legacy wallet to a PQC secure wallet. Even still, previous transactions recorded to the blockchain using the legacy wallet remain vulnerable to HNDL's data privacy risks. Second, forcing the full network to a new PQC and cryptographically agile hard fork would also not retroactively protect the privacy of historical Bitcoin transaction data with only a hard fork and *future* crypto agility, with the difficulty possibly increasing alongside a transaction's relative age. A bad actor storing a current replica of the Bitcoin ledger may need only wait long enough to obtain access to a sufficiently powerful quantum computer to reveal the ledger's cryptographically obscured transaction data, making Mosca's Theorem the dominant, if not the only, data privacy protection should revealed data no longer be relevant by the time it becomes vulnerable. Yet, that determination is up to the payors, payees, and network users whose data privacy becomes vulnerable to a quantum computer. Data thought to be protected by blockchain hashing and cryptographic techniques could be revealed in some amount of detail, including plain text, diminishing the data privacy of a distributed network's previous transactions. A bad actor would have access to view private keys and transaction data that users likely intended to be kept confidential.

5 Conclusion

The HNDL risk is active in networks currently employing traditional cryptography. The privacy of data recorded in these networks is theoretically vulnerable to a sufficiently powerful quantum computer in time. We note a particular threat to data privacy for permissionless and decentralized distributed ledger networks reliant upon traditional cryptography. We do not currently see sufficient mitigations to HNDL's data privacy risks for distributed ledger networks, although mitigations exist that could curb HNDL's security, data integrity, and theft risks. We hold that the poorly mitigated HNDL data privacy risk for DLT networks may allow a bad actor(s) to obtain a currently protected copy of a blockchain network's distributed ledger, purposefully store it in a non-PQC manner, and, irrespective of POC mitigations deployed within the distributed ledger network, in the fullness of time use a sufficiently powerful quantum computer to break the vulnerable cryptographic protections of the stored ledger replica. Given the ability of existing proposals to mitigate theft, security, and integrity risks, we look to future research to propose thorough mitigations for the data privacy risks posed by the HNDL threat to distributed ledger networks.

References

"Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger Journal,* vol. 3, pg. 69. https://ledger.pitt.edu/ojs/ledger/article/view/127/107.

Badev, Anton, and Matthew Chen (2014). "Bitcoin: Technical Background and Data Analysis," Finance and Economics Discussion Series 2014-104, Board of Governors of the Federal Reserve System. www.federalreserve.gov/econresdata/feds/2014/files/2014104pap.pdf.

Barmes, Itan, Bram Bosch, and Olaf Haalstra. "Quantum Computers and the Bitcoin Blockchain," Deloitte Netherlands, n.d., www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html.

Bitcoin Project. Accessed 2025. "Running A Full Node," Bitcoin.org, https://bitcoin.org/en/full-node#minimum-requirements.

Bank for International Settlements (2023). "Quantum-proofing the financial system," Project Leap, BIS Innovation Hub (June). https://www.bis.org/publ/othp67.pdf.

Buterin, Vitalik (2023). "How to Hard Fork to Save Most Users' Funds in a Quantum Emergency," Ethereum Research (March). www.ethresear.ch/t/how-to-hard-fork-to-save-most-users-funds-in-a-quantum-emergency/18901.

Choy, Eric (2024). "Understanding the Differences Between Bitcoin Address Formats When Developing Your App." Hiro (August 23). https://www.hiro.so/blog/understanding-the-differences-between-bitcoin-address-formats-when-developing-your-app#what-is-a-bitcoin-address.

Cruz, Agustin (2025). "Bitcoin QR Hash," Bitcoin-dev, Google Groups (11 February). www.groups.google.com/g/bitcoindev/c/8PM6iZCeDMc.

Cryptoquick (2024). "BIP: Pay-to-QR-Hash (P2QRH)," GitHub (June 8). github.com/cryptoquick/bips/blob/e186b52cff5344c789bc5996de86697e62244323/bip-p2qrh.mediawiki.

Encrypthos (2025). "Harvest Now Decrypt Later," Encrypthos (May 10). https://encrypthos.com/term/harvest-now-decrypt-later/.

Febrero-Bande, Manuel, Wenceslao Gonzalez-Manteiga, Brenda Prallon, and Yuri F. Saporito (2022). "Functional Classification Methods for Bitcoin Blockchain Data," arXiv (18 July). arxiv.org/pdf/2202.12019.

Gidney, Craig (2025). "How to factor 2048 bit RSA integers with less than a million noisy qubits," ArXiv (May 21). [2505.15917] How to factor 2048 bit RSA integers with less than a million noisy qubits.

Hunt, James (2024). "Here's What Satoshi Said to Do If Quantum Computing Cracks Bitcoin," The Block (December 10). www.theblock.co/post/330108/heres-what-satoshi-said-to-do-if-quantum-computing-cracks-bitcoin.

ITU-T (2023). “Guide Technical Report. lines for quantum-safe distributed ledger technology systems.” Technical report, International Telecommunication Union (ITU) Publications (September). https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2023-5-PDF-E.pdf

Ivezic, Martin (2025). “Breaking RSA Encryption: Quantum Hype Meet Reality (2022-2025),” Post Quantum, (April 2). https://postquantum.com/post-quantum/breaking-rsa-quantum-hype/.

Katz, Jonathan, and Yehuda Lindell (2014). *Introduction to Modern Cryptography*, 2nd ed., Chapman and Hall/CRC.

Lerman, Rachel, and Matt O’Brien (2019). “Google claims quantum computing milestone. IBM pushes back,” PBS News (October 23). https://www.pbs.org/newshour/science/google-claims-quantum-computing-milestone-ibm-pushes-back.

Litinski, Daniel (2023). “How to compute a 256-bit elliptic curve private key with only 50 million Toffoli gates,” ArXis (June 14). https://arxiv.org/abs/2306.08585.

Mascelli, Jillian (2023). “Data Privacy for Digital Asset Systems,” Finance and Economics Discussion Series 2023-059. Board of Governors of the Federal Reserve System, https://www.federalreserve.gov/econres/feds/data-privacy-for-digital-asset-systems.htm or https://doi.org/10.17016/FEDS.2023.059.

Moody, Dustin, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper (2024). “Transition to Post-Quantum Cryptography Standards,” NIST (November). https://nvlpubs.nist.gov/nistpubs/ir/2024/NIST.IR.8547.ipd.pdf

Moody, Dustin, comment in paper during review made in July 2025.

Mosca, Michele, and Marco Piani (2024). “Quantum Threat Timeline Report,” Global Risk Institute (December 6). https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/.

Murgia, Madhumita, and Richard Waters (2019). “Google claims to have reached quantum Supremacy,” Financial Times (September 20). https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17

NIST (2024). “NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” NIST (August 13). https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards.

NIST (2025a). “NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption,” NIST (March 11). https://www.nist.gov/news-events/news/2025/03/nist-selects-hqc-fifth-algorithm-post-quantum-encryption.

NIST (2025b). “Quantum Computing Explained,” NIST (March 24). https://www.nist.gov/quantum-information-science/quantum-computing-explained.

NIST (2025c). “What Is Post Quantum Cryptography?” NIST (June 11). https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

NIST (2025d). “What is Quantum Cryptography?” NIST (May 19). https://www.nist.gov/cybersecurity/what-quantum-cryptography.

NIST (2022). “Quantum Logic Gates,” NIST (April 5). https://www.nist.gov/physics/introduction-new-quantum-revolution/quantum-logic-gates.

Okta (2024). “RSA Encryption: Definition, Architecture, Benefits & Use,” Okta (August 30). https://www.okta.com/identity-101/rsa-encryption/.

PayPal (2024). "Accept Crypto Payments." PayPal Business Resource Center (August 2024), accessed 2025. https://www.paypal.com/us/brc/article/accept-crypto-payments.

Scholten, T., Williams, C., Moody, D., Mosca, M., Hurley, W., Zeng, W., Troyer, M. and Gambetta, J. (2024). “Assessing the Benefits and Risks of Quantum Computers,” IEEE Security & Privacy. https://arxiv.org/pdf/2401.16317.

Susskind, Leonard, and Art Friedman (2015). *Quantum Mechanics: The Theoretical Minimum*. Basic Books, 2015.

Swayne, Matt (2025). “Quantum Computing Roadmaps: A Look at the Maps and Predictions of Major Quantum Players,” Quantum Insider (May 23). Quantum Computing Roadmaps: A Look at The Maps And Predictions of Major Quantum Players.

Swayne, Matt (2024). “12 Top Quantum Computing Universities In 2024,” Quantum Insider (May 28). https://thequantuminsider.com/2022/04/18/the-worlds-top-12-quantum-computing-research-universities/

Zitter, Leah (2025). “What is quantum computing? How it works and examples,” Tech Target (June 24). https://www.techtarget.com/searchcio/definition/quantum-circuit.