Quantum Computing Threat on the Pseudonymity of Bitcoin
David Zebedee Kleinsorge
December 11, 2025

Abstract

Advances in quantum computing pose a unique threat to Bitcoin's long-term privacy features. Recent attention from institutions such as the United States Federal Reserve underscores the urgency of these risks, warning that quantum capabilities may eventually expose historical Bitcoin transactions to retroactive deanonymization.[1] This paper provides a technical overview of Bitcoin's cryptographic architecture and its reliance on elliptic curve digital signatures, showing how quantum algorithms, particularly Shor's algorithm, could break these primitives and theoretically allow adversaries to link public keys to real-world identities. After outlining the mechanics and feasibility of such attacks, the paper examines the ethical implications of participating in a monetary system whose privacy assurances may fail in hindsight. These questions are framed through the ethical defense of Bitcoin offered in *Resistance Money* by Andrew Bailey, Bradley Rettler, and Craig Warmke, whose work emphasizes privacy as a core moral feature of digital monetary systems.[2] Quantum-driven privacy risks are not merely technical concerns but constitute morally urgent challenges for decentralized finance.

I. Introduction

The modern digital landscape is built on an uneasy dependence: individuals, institutions, and entire economies now rely on technical systems that few thoroughly understand. Privacy, once a clear-cut position, has become a complex and fragile resource mediated by layers of

[1] Mascelli, Jillian, and Megan Rodden. "“Harvest Now Decrypt Later”: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks." *Finance and Economics Discussion Series* 2025-093, Federal Reserve Board. (2025)

[2] Andrew M. Bailey, Bradley Rettler, and Craig Warmke, *Resistance Money: A Philosophical Case for Bitcoin* (Routledge, 2024).

cryptographic infrastructure. Among the technologies that emerged in response to these pressures, Bitcoin occupies a distinctive place. In 2008, Satoshi Nakamoto introduced a form of financial autonomy insulated from centralized oversight, offering users the possibility of transacting without surrendering control over their personal information.[3] Yet this promise is only as strong as the cryptographic assumptions that make it possible.

These assumptions are under threat. Quantum computing, once a distant theoretical horizon, is rapidly developing into a credible threat to classical cryptography. Of particular concern is the harvest-now, decrypt-later (HNDL) model of attack, in which an adversary collects publicly available data today and waits until future quantum machines can break the cryptographic primitives securing it. The relevance of this threat is no longer speculative; a recent publication by the United States Federal Reserve explicitly warns that quantum capabilities may ultimately expose Bitcoin users to retroactive privacy failures, with the potential to reveal decades of transactional history in a single computational leap.[4]

The prospect of such a collapse raises pressing technical and ethical questions. A system widely promoted as privacy-preserving may harbor vulnerabilities capable of undermining that privacy long after users believed their information was safe. The permanence of a public ledger amplifies this risk: once data is recorded on a blockchain, by design it cannot be erased. The ethical landscape shifts not only when privacy fails, but even when its technical foundations become uncertain. When users cannot reliably know whether the mechanisms securing their anonymity will withstand future breakthroughs, their consent becomes compromised, and the

[3] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008).

[4] Mascelli, Jillian, and Megan Rodden. ““Harvest Now Decrypt Later”: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks.” *Finance and Economics Discussion Series* 2025-093, Federal Reserve Board. (2025)

moral justification for encouraging or participating in such a system becomes less clear. The mere possibility of retroactive exposure forces a reevaluation of Bitcoin's privacy claims and the responsibilities borne by those who design, maintain, and endorse the system.

To assess the significance of this threat, the paper begins with a technical examination of Bitcoin's cryptographic architecture, with special emphasis on elliptic curve digital signatures and the mechanisms by which public keys become exposed on-chain. It then analyzes how quantum algorithms destabilize these foundations, setting the stage for attacks that could retroactively deanonymize users. Once this framework is established, we turn to the ethical implications to evaluate what it means to participate in a monetary system whose privacy guarantees may not endure.

II. Bitcoin's Cryptographic Architecture and Privacy Foundations

Bitcoin's privacy model is based on its underlying cryptographic architecture. At its core, Bitcoin functions as a distributed ledger that records transactions publicly while relying on cryptographic mechanisms to prevent users' real-world identities from being trivially inferred. The system's security and pseudonymity emerge from an orchestration of public-key cryptography, hashing functions, digital signatures, and a consensus protocol that validates transactions without requiring trust in any central authority.[5] Understanding these components is essential for evaluating how fragile Bitcoin's privacy becomes when the computational assumptions behind them are threatened.

The most important element of Bitcoin's privacy architecture is its use of public-key cryptography, specifically the Elliptic Curve Digital Signature Algorithm (ECDSA). Each

[5] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008).

Bitcoin user controls one or more private keys and derives corresponding public keys used to authorize transactions.[6] These public keys are then hashed into shorter, more manageable addresses, which users share to receive funds. This two-step transformation (public key → hash → address) adds a thin but powerful layer of abstraction, making it more difficult to link a specific address back to a known public key. But this protection is conditional: whenever a user spends funds, their public key is revealed as part of the transaction's unlocking script.[7] At that moment, the privacy provided by hashing dissolves, and the long-term confidentiality of the user's financial activity depends entirely on the cryptographic hardness of ECDSA.

Bitcoin's pseudonymity—the idea that users transact using identifiers not directly tied to their legal names—does function as a real privacy feature, but it is far from perfect. While Bitcoin does not encode real-world identities, the public and permanent nature of the blockchain allows observers to track the flow of funds, analyze address clusters, and identify behavioral patterns.[8] Substantial work in blockchain forensics has shown that, with sufficient auxiliary information (e.g. exchange records or network-layer metadata) transactional identities can often be inferred.[9] To account for this, Bitcoin supports additional tools such as CoinJoin and the Lightning Network, which obscure transaction flows by pooling inputs or routing payments off-chain. Still, these mechanisms introduce their own limitations—including participation constraints, network surveillance risks, and practical frictions—meaning that while they enhance

[6] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore, "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives* 29, no. 2 (2015): 213–238.

[7] Jillian Mascelli and Megan Rodden, "'Harvest Now Decrypt Later': Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," Finance and Economics Discussion Series 2025-093 (Federal Reserve Board, 2025). 11-12

[8] Phillip Koshy, Diana Koshy, and Patrick McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Data," in *Financial Cryptography and Data Security*, 469–485 (Springer, 2014).

[9] Lasse Herskind, Panagiota Katsikouli, and Nicola Dragoni, "Privacy and Cryptocurrencies—A Systematic Literature Review," *IEEE Access* 8 (2020): 54044–54059.

privacy, they do not fully resolve the structural vulnerabilities inherent in a public ledger.[10] While imperfect, Bitcoin's pseudonymity generally does subsist: most users are not trivially deanonymized, and privacy failures usually require targeted analysis rather than automatic disclosure.

The durability of Bitcoin's privacy also depends on cryptographic primitives that ensure the authenticity and immutability of transactions. Digital signatures allow users to prove ownership of funds without revealing their private keys, while one-way hash functions ensure that transaction data and block histories cannot be manipulated without detection. The combination of hashing and digital signatures creates a ledger in which the data is public, but the ability to alter or impersonate transactions is computationally infeasible. The system's aspirations to privacy therefore hinge on the continued validity of the assumptions behind ECDSA and related primitives—assumptions that are intentionally abstracted away from user visibility.

Importantly, Bitcoin's privacy model is layered by the fact that public keys are not always exposed immediately. In standard practice, only addresses (hashes of public keys) appear on-chain until the first time those coins are spent, at which point the full public key is revealed.[11] This staggered exposure means that Bitcoin's privacy is time-variant: some keys are hidden, others are fully visible, and once revealed, they remain visible forever. This distinction becomes crucial when considering attacks that exploit future computational advances to derive private keys from publicly exposed material. As several authors note, Bitcoin's long-term security depends critically on the continued hardness of the Elliptic Curve Discrete Logarithm Problem

[10] Andrew M. Bailey, Bradley Rettler, and Craig Warmke, *Resistance Money: A Philosophical Case for Bitcoin* (New York: Routledge, 2024), 126-134

[11] Jillian Mascelli and Megan Rodden, "'Harvest Now Decrypt Later': Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," Finance and Economics Discussion Series 2025-093 (Federal Reserve Board, 2025). 11-12

(ECDLP, the problem underlying ECDSA), since an efficient quantum algorithm would allow a sufficiently large quantum computer to derive private keys from exposed public keys, rendering ECDSA signatures effectively insecure.[12]

Finally, the permanence of blockchain data amplifies the ethical stakes of Bitcoin's cryptographic design. Once a transaction is embedded in the blockchain, it cannot be deleted or amended. This immutability—one of Bitcoin's defining features—means that any future cryptographic weakness has retrospective force. A vulnerability discovered decades later could expose the full history of a user's activity, regardless of the privacy expectations they held at the time the transactions were made. Although this risk is widely acknowledged in high-level discussions of blockchain security, the literature lacks a comprehensive evaluation of its ethical implications—an evaluative gap that later sections of this paper aim to fill. The next section will establish and evaluate the technical aspects of the quantum threat.

III. The Threat of Quantum Computing

The technical foundations of Bitcoin's privacy model rely on assumptions about what kinds of computations are feasible for an adversary. Classical cryptography treats certain mathematical problems as effectively intractable because solving them would require astronomical amounts of computational effort. This assumption has held throughout the digital era. But quantum computing represents a categorical shift in computational capability—one that calls these hardness assumptions into question. To understand why, and what this means for Bitcoin, we must briefly examine how quantum computers differ from classical computers, how

[12] Divesh Aggarwal, Gavin Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger* 3 (2018).

their strengths interact with the elliptic curve signatures used in Bitcoin, and how realistic the timeline for quantum disruption actually is.

Quantum computers operate on quantum bits, or qubits, which differ fundamentally from classical bits. A classical bit stores a single value—0 or 1. A qubit, by contrast, exists in a superposition of states, capable of representing both 0 and 1 simultaneously with complex amplitudes. When multiple qubits are entangled, their joint state cannot be described independently; instead, the computational state grows exponentially with the number of qubits. This property allows quantum computers to evaluate a vast number of possibilities in parallel, not by brute force, but by exploiting interference patterns in quantum state evolution. The challenge is stability: qubits are extraordinarily sensitive to noise and decoherence. Error correction requires substantial overhead, meaning that a "logical," stable qubit requires many more physical qubits to sustain coherence over time.[13]

Bitcoin's security depends heavily on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Bitcoin specifically relies on the secp256k1 elliptic curve, a Koblitz curve defined over a 256-bit finite field that is optimized for fast computation and compact keys but does not have any known backdoors or structural weaknesses under classical analysis[14] (in contrast with the National Institute of Standards and Technology's Dual EC DRBG[15]). Without cutting too deep, the problem is simple to state: given a generator point G on an elliptic curve and a public key $Q = kG$, determine the private key k. For classical computers,

[13] Bilal Shaw et al., "Encoding One Logical Qubit into Six Physical Qubits," *Physical Review A* 78, no. 1 (2008): 012337.
[14] Joppe W. Bos et al., "Elliptic Curve Cryptography in Practice," in *International Conference on Financial Cryptography and Data Security* (Berlin: Springer, 2014), 157–75.
[15] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen, "Dual EC: A Standardized Back Door," in *The New Codebreakers*, ed. Peter Ryan, David Naccache, and Jean-Jacques Quisquater, vol. 9100 of *Lecture Notes in Computer Science* (Berlin: Springer, 2016), 256–81

no efficient algorithm is known, and the best attacks require time on the order of the square root of the curve's order—far beyond feasible search bounds. This is analogous, conceptually, to Bitcoin's mining difficulty: both rely on the asymmetry between how hard it is to verify a solution (easy) and how hard it is to find one (computationally intractable). So long as ECDLP remains hard, public keys cannot be leveraged to derive private keys, and Bitcoin's pseudonymous architecture remains intact.

In the 1990s, however, Peter Shor introduced a quantum algorithm capable of solving integer factorization and discrete logarithm problems in polynomial time.[16] Applied to elliptic curves, Shor's algorithm transforms ECDLP from an intractable search problem into one that a sufficiently large quantum computer could solve efficiently. Although ECDSA signatures obfuscate private keys under classical assumptions, Shor's algorithm implies that once a public key is exposed—whether through address reuse, multisignature conditions, or script operations—a quantum-enabled adversary could derive the underlying private key and impersonate the signer.

The critical question, then, is not whether Shor's algorithm threatens Bitcoin in principle, but when quantum computers will achieve the scale, coherence, and error-corrected stability necessary to run it at the sizes required to break secp256k1. Many cryptographers argue that running Shor's algorithm on Bitcoin's curve would require millions of physical qubits, given the overhead for quantum error correction.[17] Others suggest that advances in surface codes, cryogenic architectures, and qubit connectivity may reduce this threshold substantially, though

[16] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," *SIAM Review* 41, no. 2 (1999): 303–32.
[17] Enrique Martin-Lopez et al., "Experimental Realization of Shor's Quantum Factoring Algorithm Using Qubit Recycling," *Nature Photonics* 6, no. 11 (2012): 773–76.

these predictions remain speculative.[18] What is clear is that the gap between theoretical and practical capability remains large. Current machines operate with hundreds of noisy qubits—impressive from a scientific standpoint but orders of magnitude below what is required for breaking ECDSA at scale.[19]

Still, timelines matter ethically even when they remain uncertain technically. A breakthrough in scalable qubit coherence or error correction could shift expectations rapidly. In this sense, the relevant timeline is not when quantum computers will be able to break ECDSA, but when the possibility that they might becomes operationally significant for adversaries engaged in long-term data harvesting. The implications of this technical landscape set the stage for the next section. If quantum computing threatens the hardness assumptions that secure Bitcoin's privacy, then we must examine not only the mathematical vulnerability but also what practical attack scenarios emerge from it. The following section turns from the structure of the threat to the mechanics of exploitation, evaluating how a quantum-enabled adversary could leverage harvested data, network surveillance, and protocol features to unravel Bitcoin's privacy model in practice.

IV. Vulnerabilities of Bitcoin's Privacy Model

Much of the existing literature identifies the broad contours of the harvest-now, decrypt-later (HNDL) attack model: ECDSA becomes breakable once sufficiently powerful quantum computers exist[20], and any encrypted or cryptographically protected data harvested

[18] Emanuel Knill, "Quantum Computing with Realistically Noisy Devices," *Nature* 434, no. 7029 (2005): 39–44.

[19] Jay Gambetta, "Expanding the IBM Quantum Roadmap to Anticipate the Future of Quantum-Centric Supercomputing," *IBM Research Blog*, 2022.

[20] Divesh Aggarwal, Gavin Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel, "Quantum Attacks on Bitcoin, and How to Protect Against Them," *Ledger* 3 (2018).

today may be decrypted years or decades later.[21] Our task in this section is to examine these claims by walking through concrete adversarial scenarios and considering how the threat evolves as we introduce additional aspects of Bitcoin's architecture and usage patterns. Beginning with the simplest case and gradually adding layers of complexity will allow us to see how quantum attacks affect Bitcoin's privacy model—sometimes weakening it dramatically, sometimes being partially mitigated, but ultimately revealing the structural vulnerabilities.

Consider a simple scenario in which a user spends funds from a legacy Bitcoin address. Spending from such an address reveals the user's public key on-chain. Under classical cryptography, this exposure is harmless; the ECDLP is believed to be intractable at Bitcoin's parameter sizes.[22] Under an HNDL model, however, a well-resourced adversary records the entire blockchain today and waits until quantum computers capable of running Shor's algorithm at scale become available.[23] At that point, any exposed public key can be used to compute its underlying private key. Even this minimal scenario already results in a profound privacy failure: once a single private key is recovered, the attacker can reconstruct every transaction ever made *with that key*, link it to address clusters, and potentially unwind significant portions of the user's financial history.[24]

This baseline case becomes more troubling once we add behavioral data. Many early Bitcoin users reused addresses or relied on older address formats. These legacy and reused

[21] Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and National Institute of Standards and Technology (NIST), *Quantum-Readiness: Migration to Post-Quantum Cryptography* (CISA Tech. Rep., 2023).
[22] Claus Diem, "On the Discrete Logarithm Problem in Elliptic Curves," *Compositio Mathematica* 147, no. 1 (2011): 75–104.
[23] Vaishali Bhatia and K. R. Ramkumar, "An Efficient Quantum Computing Technique for Cracking RSA Using Shor's Algorithm," in *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 89–94 (IEEE, 2020).
[24] Lasse Herskind, Panagiota Katsikouli, and Nicola Dragoni, "Privacy and Cryptocurrencies—A Systematic Literature Review," *IEEE Access* 8 (2020): 54044–54059.

addresses are disproportionately vulnerable, both because they rely on earlier cryptographic constructions and because address reuse provides adversaries with richer behavioral information to exploit.[25] A single key recovery in such cases does not merely deanonymize one payment; it deanonymizes a long sequence of actions, revealing temporal patterns, recurring counterparties, and possibly even economic relationships. The immutable nature of the blockchain ensures that all this data remains available indefinitely, waiting for a future cryptographic breakthrough to render it intelligible.

Bitcoin users can employ privacy-enhancing techniques such as CoinJoin to obscure the relationship between inputs and outputs. CoinJoin enables users to sever links between their prior transaction histories and subsequent activity by constructing joint transactions without relying on a trusted intermediary.[26] At first glance, this appears to significantly mitigate the privacy harms identified above. Yet quantum attacks introduce a subtle risk: if a user participates in a CoinJoin transaction and later has one of their public keys recovered by a quantum adversary, the attacker may be able to reduce the CoinJoin anonymity set by analyzing the structure of the transaction or correlating on-chain behavior with patterns known from harvested data. CoinJoin obscures certain relationships, but it does not eliminate the structural vulnerability created by exposed public keys—and quantum computing magnifies that vulnerability by making key recovery feasible rather than merely theoretical.

Lightning presents a different kind of complexity. It offers substantial privacy improvements by routing payments through off-chain channels where only intermediary nodes

[25] Jillian Mascelli and Megan Rodden, "'Harvest Now Decrypt Later': Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks," *Finance and Economics Discussion Series* 2025-093 (Federal Reserve Board, 2025).
[26] Andrew M. Bailey, Bradley Rettler, and Craig Warmke, *Resistance Money: A Philosophical Case for Bitcoin* (New York: Routledge, 2024), 126–131.

witness the transaction path.[27] This privacy model presupposes the secrecy of communication channels and the integrity of the key-exchange protocols used to establish connections. An HNDL-capable adversary who records Lightning traffic today could later decrypt this information if the underlying public-key mechanisms used in channel establishment remain quantum-vulnerable. Once decrypted, previously hidden routing paths and channel relationships may become visible. Even partial visibility can allow an attacker to link Lightning activity to particular IP addresses or to correlate off-chain spending with subsequent or prior on-chain channel updates. Thus, Lightning improves privacy under classical assumptions, but its guarantees degrade sharply once communication metadata becomes retroactively decryptable.

The most severe privacy failures arise when HNDL attacks are paired with long-term network surveillance. Mascelli and Rodden suggest that Bitcoin's pseudonymous identifiers are not subject to HNDL privacy risks because they are already public[28], but this claim only holds if public pseudonyms remain isolated from other data sources. In reality, pseudonyms become problematic when they can be linked to identity-bearing information harvested from encrypted communication channels. Consider an adversary who records large volumes of TLS-encrypted traffic between users and centralized exchanges or wallet services today. Under classical assumptions, this data appears opaque; in a post-quantum world, those TLS sessions could be decrypted[29], revealing login credentials, withdrawal requests, account identifiers, and

[27] Bailey, Rettler, and Warmke, *Resistance Money*, 131-133

[28] Mascelli, Jillian, and Megan Rodden. "“Harvest Now Decrypt Later”: Examining Post-Quantum Cryptography and the Data Privacy Risks for Distributed Ledger Networks." *Finance and Economics Discussion Series* 2025-093, Federal Reserve Board. (2025), 16

[29] Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and National Institute of Standards and Technology (NIST), *Quantum-Readiness: Migration to Post-Quantum Cryptography* (CISA Tech. Rep., 2023).

timestamps. When these decrypted sessions are correlated with on-chain deposit and withdrawal events, an adversary can begin to map specific pseudonyms to real-world identities.

The same concern applies to peer-to-peer network traffic more generally. Research has shown that correlating transaction announcements with network routing data can significantly aid deanonymization, especially when combined with IP-level observation.[30] If a quantum adversary records encrypted P2P traffic today and later decrypts it, the adversary may retroactively identify which IP address originated which transaction. Combined with ISP logs or other harvested metadata, these links could become extraordinarily revealing. Thus, public pseudonymous identifiers are not privacy-neutral; they become the anchoring coordinates of a retroactive deanonymization system once the surrounding protective cryptography collapses.

Bringing these elements together, a fully enriched HNDL attack illustrates how deeply quantum vulnerability is woven into Bitcoin’s privacy model. An attacker who harvests the blockchain, captures network traffic, stores encrypted communications, and waits for quantum breakthroughs gains the ability to reconstruct a user's financial life in extraordinary detail. Key recovery exposes past signatures; decrypted network traffic links pseudonyms to IP addresses and accounts; transaction graph analysis spreads those linkages outward; and both CoinJoin and Lightning provide only partial barriers. The result is not merely a threat to individual transactions but a threat to the long-term confidentiality of entire user histories.

This technical picture sets the stage for the normative questions to follow. If quantum-enabled adversaries can retroactively decode the transactional and communicative history of Bitcoin users, then Bitcoin’s ethical foundations—its promises of autonomy,

[30] Phillip Koshy, Diana Koshy, and Patrick McDaniel, “An Analysis of Anonymity in Bitcoin Using P2P Network Data,” in *Financial Cryptography and Data Security*, 469–485 (Springer, 2014).

censorship resistance, and non-domination—must be reevaluated. In the next section, we assess whether Bitcoin can still satisfy the privacy-centered moral claims commonly made in its defense, and how quantum-era vulnerabilities reshape the normative landscape.

V. Ethical Implications of Privacy Instability

Privacy entails far more than the concealment of facts or actions. It concerns a fundamental kind of control. Specifically, the capacity of individuals to manage how they are perceived by others and to regulate what personal information is shared, to whom, and under what circumstances. Philosophers and legal theorists often distinguish between two central forms of privacy: privacy from access and privacy as control. On the access view, privacy is violated when an outsider non-consensually accesses personal information. On the control view, privacy is violated when a party exercises control over one's personal information—whether or not it has been accessed. In earlier eras, these domains typically aligned: to be physically unavailable was often to be informationally secure. But digital infrastructure has fractured this alignment. Today, surveillance extends beyond physical space; it is embedded in software, inferred from metadata, and compiled continuously across platforms. Digital systems increasingly produce mechanisms that allow their users to be authenticated while obfuscating identifiable information.

Bitcoin enters this landscape presenting itself as a restorative force for both access and control privacy. Even though the ledger is public, encryption and pseudonymity prevent outsiders from accessing private information or linking identities to transactions, preserving a meaningful layer of access privacy. At the same time, because the system enables users to hold and transfer value without intermediaries, it also provides control privacy: users determine how much personal financial information is revealed, and to whom. Because Bitcoin allows users to transact without linking identities to addresses, the system enables a unique hybrid of transparency and anonymity. Bitcoin's appeal as a liberatory financial technology draws much of its force from this promise: that it can secure both forms of privacy at once, offering transparency without exposure.[31]

As discussed, this vision relies on a crucial assumption: that Bitcoin's cryptographic foundations will remain durable. Quantum computing disrupts that assumption. A user may believe their financial activity is shielded by pseudonymity, only to discover long after the fact that their transaction history has been retroactively exposed. The blockchain's immutability becomes, in this context, a mechanism for indefinite vulnerability. This realization profoundly alters the ethical landscape. If Bitcoin's privacy is contingent rather than stable, then the moral justification for using, promoting, or defending the system requires reevaluation. Retroactive privacy loss is not a minor inconvenience; it strikes at the very concept of privacy itself. When information that was once shielded can be exposed years later, the basic expectation of informational control collapses. Privacy of control depends on the ability to decide what others can learn about one's actions, and when. Unlike traditional data breaches, which may be patchable or containable, the public ledger ensures that once deanonymization occurs, it does so universally and irreversibly.

Questions about responsibility follow naturally. Encouraging people to use a system that archives their financial behavior forever—and whose privacy guarantees may dissolve—raises concerns about informed consent and moral risk. Bitcoin is not a purely technical artifact; it

[31] Finn Brunton, "Recognizable without Being Known," in *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency* (Princeton, NJ: Princeton University Press, 2019), 33–46.

expresses and depends upon social beliefs about governance, trust, and economic infrastructure.[32] One might object that centralized digital money is hardly safer, since banks and payment processors also store detailed, long-lasting records of financial activity. But these systems face a *theoretical* risk of breach or institutional misconduct; their records are not destined for de-anonymization by a future mathematical breakthrough. By contrast, the quantum threat makes a certain kind of privacy loss *functionally guaranteed* for any data that has been stored in encrypted form today. This places Bitcoin in a categorically different position: the failure mode is not a contingent institutional lapse but a predictable structural outcome of technological progress. If Bitcoin users cannot meaningfully evaluate the risks posed by quantum decryption, then their consent to its privacy model is, at best, incomplete.

Craig Warmke's reflections on the conceptual structure of Bitcoin reinforce this point. What counts as a "coin," how ownership is represented, and how value is tracked are all matters of abstraction rather than physical referents.[33] If users already misunderstand Bitcoin's conceptual scaffolding, it is unsurprising that they may also misunderstand the fragility of the privacy built atop it. Consent, in such a case, is compromised not by deception but by structural opacity: the system requires users to trust cryptographic properties whose longevity they cannot assess.

This reorientation has implications for decentralized finance more broadly. Its normative appeal depends on the durability of its protections. If privacy is temporary, then such systems may offer comfort without security—shielding users today only to expose them tomorrow. Unlike traditional financial institutions, Bitcoin has no central authority capable of redacting,

[32] Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore, "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives* 29, no. 2 (2015): 213–238.
[33] Craig Warmke, "Electronic Coins," 2022.

overwriting, or destroying historical records. Bitcoin has facilitated illicit activity precisely because users perceive it as anonymous.[34] But if that perceived anonymity dissolves under quantum attack, the consequences will extend beyond criminals to activists, dissidents, and ordinary individuals who relied on pseudonymity as a safeguard. Bailey, Rettler, and Warmke present a compelling moral defense of Bitcoin. But that defense rests on the assumption that the privacy Bitcoin affords is not only meaningful but resilient. In a world where quantum decryption is plausible and transactional records are permanent, this assumption must be critically reassessed. Without durable privacy, Bitcoin may still function as a monetary technology. But it cannot, in the way these authors suggest, function as an ethically exceptional one.

VI. Reassessing Bitcoin

This paper has examined the vulnerability of Bitcoin's privacy guarantees in a prospective quantum era, arguing that the risks posed by harvest-now, decrypt-later (HNDL) attacks are not merely technical curiosities but ethically significant faults in the moral case for Bitcoin. The analysis proceeded in three steps. First, it laid out Bitcoin's cryptographic and architectural foundations, especially its reliance on elliptic curve digital signatures and the pseudonymous structure of its public ledger. Second, it evaluated how quantum computing and HNDL strategies threaten those foundations, not only at the level of key recovery but in conjunction with network surveillance and long-term data harvesting. Finally, it examined how these technical risks bear on the ethical justification of Bitcoin. Taken together, these strands support a central conclusion: Bitcoin's ethical status as a privacy-protecting technology is

[34] David Yaffe-Bellany, Spencer Woodman, and Sam Ellefson, "The Crypto Industry's $28 Billion in 'Dirty Money'," *New York Times*, 2025.

contingent on cryptographic assumptions that are increasingly uncertain, and this contingency must figure prominently in any responsible moral evaluation of the system.

Technically, Bitcoin’s privacy architecture is fragile. The system’s pseudonymity arises from the combination of public-key cryptography, hash-based addresses, and a validation mechanism that allows value to move without linking addresses directly to legal identities. In the classical setting, ECDSA over secp256k1 provides both integrity and a kind of indirect confidentiality: external observers can see that funds moved, to and from which addresses, but cannot feasibly infer which individuals control those addresses. Privacy, in this sense, is an emergent property of hardness assumptions: as long as the Elliptic Curve Discrete Logarithm Problem remains computationally intractable, exposed public keys do not automatically translate into compromised identities. Bitcoin’s immutability and openness are, under these assumptions, compatible with a meaningful degree of privacy from access and privacy as control.

Quantum computing destabilizes this equilibrium by attacking the cryptographic substrate rather than the protocol’s high-level logic. Shor’s algorithm, implemented on a sufficiently large universal quantum computer, renders ECDLP efficiently solvable, turning every exposed public key into a potential private-key oracle. HNDL attacks capitalize on this by decoupling data collection from data exploitation: adversaries can harvest blockchain data, network traffic, and encrypted communications today, confident that future quantum capabilities will eventually unlock their contents. The effect on Bitcoin is twofold. At the narrow level, individual keys and legacy addresses become vulnerable to theft once quantum resources are available. At the broader level, the entire historical record becomes susceptible to deanonymization as recovered keys, decrypted sessions, and behavioral heuristics are combined to reconstruct user identities and transactional life histories. This problem deepens when HNDL attacks are considered more broadly on the network.

The analysis in §IV showed that this threat is not confined to isolated signatures or dormant addresses. It extends across the full spectrum of Bitcoin usage. Address reuse and early address formats amplify the risk by providing richer behavioral patterns for an attacker to exploit. CoinJoin and similar collaborative transactions, while privacy-enhancing under classical assumptions, can be partially undone when quantum key recovery and auxiliary data reduce the effective anonymity set. When we factor in long-term network surveillance, the picture becomes bleaker still. Pseudonymous on-chain identifiers, which might appear harmlessly public in isolation, become the anchor points for a comprehensive deanonymization apparatus once the protective cryptography around associated communications gives way.

In this sense, the HNDL threat reveals something deeper about the structure of Bitcoin's privacy model: it is temporally fragile. The system offers privacy at one point in time by assuming the persistence of certain computational barriers. But if those barriers fail, privacy does not simply degrade prospectively; it collapses retroactively. The blockchain's immutability guarantees that any future breakthrough in cryptanalysis applies backwards across the entire ledger. What appears today as a pseudonymous blob of addresses and outputs may, in the not-so-distant future, resolve into a detailed, identity-indexed financial dossier. This temporal dimension is what distinguishes quantum-driven privacy failures from ordinary data leaks: users cannot contain the damage, roll keys, or erase past records once the ledger has been globally replicated and cryptographically bound.

The ethical analysis in §V argued that this temporal fragility has serious implications for Bitcoin's moral standing, especially in light of the argument offered in *Resistance Money*. The authors treat Bitcoin's privacy as both instrumentally and intrinsically valuable. It is instrumentally valuable because it protects individuals from surveillance and coercive interference; it is intrinsically valuable because it helps secure a domain of personal life that is not subject to arbitrary scrutiny. On their view, Bitcoin's public ledger coupled with strong cryptography yields "privacy in public": a system in which transactional information is transparent enough for verification but not so transparent as to expose individuals to undue control.[35] That moral picture, however, assumes that Bitcoin's privacy is not only real but durable.

Quantum risk undermines that presupposition. If adversaries can retroactively deanonymize Bitcoin transactions, then the autonomy Bitcoin is supposed to secure becomes conditional on a technological race users do not understand and cannot influence. Under the access conception of privacy, HNDL-enabled decryption represents a delayed but nonetheless real violation: outsiders eventually gain non-consensual access to personal financial information, even if that access is temporally deferred. Under the control conception, the violation is even more stark. Users lose meaningful control over their personal information the moment they commit transactions to a ledger whose long-term opacity they cannot guarantee. Third parties—states, corporations, or criminal organizations—gain the power to decide when and how those records will be interpreted or weaponized. The core moral goods Bitcoin is supposed to advance—autonomy, non-domination, free association—are therefore placed at risk by the very permanence that makes the system function.

[35] Andrew M. Bailey, Bradley Rettler, and Craig Warmke, *Resistance Money: A Philosophical Case for Bitcoin* (New York: Routledge, 2024), chap. 6.

Moreover, the burdens of this uncertainty are not evenly distributed. Those who most rely on Bitcoin's privacy for protection (e.g. dissidents, whistleblowers, journalists in hostile regimes, marginalized groups seeking economic independence) are precisely those who stand to be harmed most severely if that privacy collapses. For them, Bitcoin is not a speculative asset or an ideological curiosity; it is, in many cases, a survival tool. If their transactional histories become legible to adversarial states or organizations in the future, the harms could include imprisonment, persecution, or violence. From this perspective, the quantum threat introduces an *intertemporal injustice*: individuals who act under one set of privacy expectations may suffer under another, long after the point at which they could take corrective action. A system that encourages such users to trust in cryptographic shields that may not endure carries a heavy moral burden.

Situating these findings in the broader context of decentralized finance and digital infrastructure reveals an even wider set of implications. Bitcoin is often treated as the paradigm case for public blockchains, and the privacy structure of many other systems is patterned on its combination of pseudonymity and transparency. If quantum computing renders these guarantees unstable, then the ethical challenge extends to any system that promises privacy through public-key cryptography and immutable logs. Organizations like NIST have already begun to articulate roadmaps for post-quantum migration, emphasizing that critical financial infrastructure must anticipate and mitigate HNDL and related threats. But even an orderly migration to post-quantum cryptography would not erase the vulnerability of historical data. The past, already written to classical systems, remains exposed.

What, then, does this paper contribute? First, it clarifies that quantum risk to Bitcoin is not only a matter of systemic integrity—double-spend attacks or governance capture—but also, and perhaps more importantly, a matter of long-term privacy and identity exposure. Second, it shows that HNDL is best understood as a compositional threat: not simply the breaking of one cryptographic primitive, but the recombination of previously distinct and obfuscated data sources—blockchain records, network traffic, off-chain communications—into a coherent portrait of user identity and behavior. Third, it argues that this compositional threat directly undermines the ethical argument that Bitcoin is a uniquely valuable protector of privacy and autonomy. A system that can, with a single technological breakthrough, transform decades of pseudonymous activity into an intelligible and actionable surveillance database cannot straightforwardly be described as a stable bulwark against intrusion.

Finally, the analysis in this paper suggests directions for both technical and ethical work going forward. On the technical side, it underscores the urgency of transitioning not only Bitcoin, but digital financial infrastructure more broadly, to post-quantum cryptographic schemes, and of designing protocols that minimize long-term linkability and data retention wherever possible. On the ethical side, it calls for a more cautious and qualified rhetoric around Bitcoin’s privacy benefits, especially in contexts where vulnerable populations are encouraged to treat it as a protective tool. Philosophers, policy makers, and technologists alike must contend with the fact that systems built on strong cryptography are not morally inert; they embed long-term bets about future adversaries and future computation. If those bets go wrong, the harms are not borne by the abstractions but by the people whose lives are inscribed, permanently, in the ledgers we build today.

Bibliography

Aggarwal, Divesh, Gavin Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel. "Quantum Attacks on Bitcoin, and How to Protect Against Them." *Ledger* 3 (2018). https://doi.org/10.5195/ledger.2018.127.

Bailey, Andrew M., Bradley Rettler, and Craig Warmke. *Resistance Money: A Philosophical Case for Bitcoin*. Routledge, 2024.

Bernstein, Daniel J., Tanja Lange, and Ruben Niederhagen. "Dual EC: A Standardized Back Door." In *The New Codebreakers*, edited by Peter Ryan, David Naccache, and Jean-Jacques Quisquater, 256–281. Lecture Notes in Computer Science, vol. 9100. Berlin: Springer, 2016. https://doi.org/10.1007/978-3-662-49301-4_17

Bhatia, Vaishali, and K. R. Ramkumar. "An efficient quantum computing technique for cracking RSA using Shor's algorithm." In *2020 IEEE 5th international conference on computing communication and automation (ICCCA)*, 89-94. IEEE, 2020.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. "Bitcoin: Economics, technology, and governance." *Journal of Economic Perspectives* 29, no. 2 (2015): 213-238.

Bos, Joppe W., J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow. "Elliptic curve cryptography in practice." In International conference on financial cryptography and data security, pp. 157-175. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

Brunton, Finn. "Recognizable without Being Known." In *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency*, 33–46. Princeton, NJ: Princeton University Press, 2019.

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and National Institute of Standards and Technology (NIST). *Quantum-Readiness: Migration to Post-Quantum Cryptography*. CISA, Tech. Rep, 2023.

Diem, Claus. "On the discrete logarithm problem in elliptic curves." Compositio Mathematica 147, no. 1 (2011): 75-104.

Gambetta, Jay. "Expanding the IBM Quantum Roadmap to Anticipate the Future of Quantum-Centric Supercomputing." IBM Research Blog. 2022.

Herskind, Lasse, Panagiota Katsikouli, and Nicola Dragoni. "Privacy and cryptocurrencies—A systematic literature review." *IEEE Access* 8 (2020): 54044-54059.

Knill, Emanuel. "Quantum computing with realistically noisy devices." Nature 434, no. 7029 (2005): 39-44.

Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In International conference on financial cryptography and data security, pp. 469-485. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

Martin-Lopez, Enrique, Anthony Laing, Thomas Lawson, Roberto Alvarez, Xiao-Qi Zhou, and Jeremy L. O'brien. "Experimental realization of Shor's quantum factoring algorithm using qubit recycling." Nature photonics 6, no. 11 (2012): 773-776.

Mascelli, Jillian, and Megan Rodden. “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, DC: Board of Governors of the Federal Reserve System, 2025.

Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).

Shaw, Bilal, Mark M. Wilde, Ognyan Oreshkov, Isaac Kremsky, and Daniel A. Lidar. "Encoding one logical qubit into six physical qubits." Physical Review A—Atomic, Molecular, and Optical Physics 78, no. 1 (2008): 012337.

Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41, no. 2 (1999): 303-332.

Warmke, Craig. “Electronic Coins.” 2022.

Yaffe-Bellany, David, Spencer Woodman, and Sam Ellefson. “The Crypto Industry’s $28 Billion in ‘Dirty Money’.” *New York Times*. (2025)