The July 4th Anomaly: An In-Depth Analysis of the 80,000 BTC Dormant Wallet Activation

Executive Summary

On and around July 4, 2025, the Bitcoin network witnessed an event of unprecedented scale and sophistication: the coordinated activation and transfer of approximately 80,000 BTC, valued at over $8.6 billion, from eight wallets that had remained dormant since 2011.[1] This movement, the largest of its kind in Bitcoin's history, immediately ignited a firestorm of speculation and analysis across the digital asset ecosystem.[3] The event presents a central and critical conflict of interpretation. On one hand, the public narrative, particularly in mainstream financial media, framed the transfers as a benign security upgrade—a prudent whale moving assets from vulnerable legacy addresses to modern, secure formats.[3] On the other hand, a deeper analysis of the on-chain evidence and surrounding digital artifacts points toward a far more alarming conclusion: a hostile takeover of the wallets, executed through a masterful combination of cryptographic exploitation and elaborate psychological warfare.

This report provides a comprehensive, multi-faceted investigation into the July 4th Anomaly. It collates and examines the verifiable on-chain data, synthesizes the competing public hypotheses, provides a detailed technical breakdown of the most plausible attack vector, and analyzes the profound, long-term implications for the Bitcoin network. The evidence presented herein—from the low-cost "canary" test on the Bitcoin Cash network that preceded the main event, to the meticulously crafted legal threats and cryptic messages embedded directly onto the blockchain, to the public demonstration of key-cracking capabilities in the months prior—weighs heavily against the theory of a simple owner-initiated transfer.

The analysis concludes that the July 4th Anomaly was most likely a successful, large-scale cryptographic heist. This event marks a pivotal moment for the digital asset landscape, shattering long-held assumptions about the security of "lost" coins

and exposing a new class of systemic risk. It demonstrates the practical application of long-theorized cryptographic attacks at scale, forcing a necessary, if unsettling, maturation in the understanding of digital risk, ownership, and security. The aftershocks of this event will challenge Bitcoin's technical roadmap, its economic models, its legal standing, and its narrative as a secure store of value, setting a powerful precedent for the future of decentralized finance.

Section I: The Unassailable Record — On-Chain Forensics

This section presents the immutable, verifiable facts of the event as recorded on the Bitcoin and Bitcoin Cash blockchains. It serves as the empirical bedrock for all subsequent analysis, establishing a clear timeline and cataloging the digital artifacts left behind by the actor. Every hypothesis and conclusion that follows is grounded in this on-chain evidence.

1.1 The Anatomy of the Event: A Chronological Reconstruction

The operation was not a singular, impulsive act but a methodical, multi-stage process executed with precision across two different blockchains. This timeline reveals a level of planning and operational security far exceeding that of a typical user or even a standard institutional transfer.

The Prelude - The BCH "Test" Transaction

The first overt action occurred not on the Bitcoin network, but on Bitcoin Cash (BCH). On July 4, 2025, approximately 14 hours before the main BTC transfers, a small transaction was executed on the BCH blockchain from at least one of the target wallets.[4] For addresses created before the 2017 Bitcoin/Bitcoin Cash fork, the private keys are identical for both chains. This allowed the actor to perform a low-cost, low-visibility "canary" test to confirm that the compromised private key was functional and could successfully sign and broadcast a transaction.

According to on-chain analysis, a key test transaction took place at 02:41:32 UTC, moving 10,000 BCH from the Bitcoin Cash equivalent of the legacy Bitcoin address 12tLs9c9RsALt4ockxa1hB4iTCTSmxj2me.[7] This step was a critical piece of operational security. It validated the exploit's success without immediately alerting the broader Bitcoin community, which monitors the BTC blockchain far more intensely than the BCH chain. This calculated verification of key access before the high-stakes main event is a hallmark of a professional, premeditated operation, not a panicked owner.[4]

The Main Event - Coordinated BTC Transfers

With the private keys confirmed to be active, the main operation on the Bitcoin network commenced. Beginning at approximately 03:43:33 UTC on July 4, 2025, a series of highly synchronized transactions began.[7] Over the subsequent hours, approximately 80,000 BTC were systematically drained from eight distinct legacy Pay-to-PubKey-Hash (P2PKH) wallets.[1] Each of these wallets, untouched for over 14 years, held a remarkably uniform amount of around 10,000 BTC, strongly suggesting a common origin or owner.[2] The transfers were executed with a precision and concurrency that points to a single entity wielding automated scripts to control all eight private keys simultaneously.[2]

The Destination - A Security Upgrade Facade

Crucially, the 80,000 BTC were not sent to known deposit addresses of cryptocurrency exchanges, a move that would have signaled an immediate intent to sell and would have likely triggered exchange-level alerts.[5] Instead, the funds were migrated from the old, legacy P2PKH addresses (which begin with a '1') to new, modern Native SegWit (Bech32) addresses (which begin with 'bc1q').[1]

On the surface, this action mimics a legitimate security upgrade. Migrating to SegWit addresses is a recommended best practice, as it provides enhanced security features, better error checking, and significantly lower future transaction fees.[9] This choice of destination provided the actor with a plausible "cover story" that the event was merely a long-overdue wallet consolidation by the original owner.[3] However, one of the destination addresses revealed a more provocative, taunting message: the vanity address

bc1qwq5geath93h0lnfsrmnwnfuck2f9ypv4ewyl4j, which contains an expletive, was used to receive funds from source address 1f1miYFQWTzdLiCBxtHHnNiW7WAWPUccr.[7] This act of defiance stands in stark contrast to the quiet prudence of a genuine security upgrade.

1.2 The Blockchain's Graffiti: Analysis of OP_RETURN Messages

A central component of the operation was the strategic use of the OP_RETURN opcode. This feature allows a small amount of arbitrary data to be embedded into a transaction, creating a public and immutable message on the blockchain. The actor used this feature to wage a psychological campaign, crafting a public narrative directly targeting the wallet owner and the wider community.[1] The messages were sent in a deliberate sequence to the dormant wallets in the days leading up to the fund transfers.

Message Sequence and Content

1. **The Claim (July 1):** The first message, sent on July 1, 2025, was a bold and aggressive legal declaration: "LEGAL NOTICE: We have taken possession of this wallet and its contents".[2] An example transaction hash for this message is 4f7c80c05fd77a9c9b180f7f6400560d1ab6cf3a4ba1b6bf7429eeeefa500a05.[7]
2. **The Ultimatum (July 1):** Just 24 minutes later, a follow-up message laid out a challenge to the true owner: "Not abandoned? Prove it by an on-chain transaction using private key by Sept 30".[2] An example transaction hash for this is e511f90160b2f189eaf0adce7221979cbc9001bc29e6c5476914d002a9d19886.[7] This message dared the owner to use their key, the only form of proof that matters on the blockchain.
3. **The Legal Facade (July 3):** The third message directed observers to an external website, professionalizing the operation: "NOTICE TO OWNER: see salomonbros.com/owner-notice".[2] An example transaction hash for this is

ba9958bca2ae46e5fdea8737fef02bca6cfe1723196917699a058c30b6f52fd8.[7]

4. **The Cryptic Signature (July 4):** The final message, sent to at least three of the wallets, was a cultural reference designed to mystify and engage the crypto community: "4 8 15 16 23 42".[2] These are the infamous, enigmatic "Lost Numbers" from the television series *Lost*, associated with themes of fate, control, and hidden knowledge. An example transaction hash is ac35cc92a1d97298c7b2a89e1f8260da61d0447c28927585baecd2bfa863aec0.[2]

This sequence was not random. It was a carefully orchestrated performance, blending legalistic intimidation with cryptic pop culture to create a multi-layered narrative. The combination of personas—a lawyer, a mystic, a punk—is indicative of a sophisticated psychological operation designed to confuse observers and control the story.

The Counterparty Dust Transaction

The initial user query specified an interest in a "Counterparty dust" transaction of 548 satoshis. Counterparty is a protocol that allows for the creation of assets and execution of smart contracts on top of the Bitcoin blockchain, often by embedding data in standard transactions. Dust refers to a tiny, often unspendable amount of cryptocurrency.[16] While the provided source materials extensively discuss the concept of dust and the use of OP_RETURN messages, they do not contain a specific, verifiable reference to a 548 satoshi Counterparty transaction connected to this event. The significance of such a transaction, were it confirmed, would be to add yet another layer of technical sophistication, demonstrating the actor's ability to communicate or embed data using multiple protocol layers on the same blockchain. Its absence from the primary public analyses suggests it may be a detail from niche forensic circles or a potential misinterpretation.

1.3 The "Salomon Brothers" Facade: Archival and Domain Analysis

The salomonbros.com website was the off-chain anchor for the actor's legalistic narrative, lending a veneer of corporate legitimacy to the operation.[2]

Domain History and Content

The domain salomonbros.com was registered on January 6, 2023, indicating long-term planning. It was updated on July 1, 2025, immediately before the OP_RETURN campaign began.[7] The specific page referenced in the blockchain message,

/owner-notice, was deployed on July 3, 2025, and was archived by the Internet Archive's Wayback Machine on July 3rd and 4th, capturing its initial state.[7]

The website itself was slick and professional, branded with the name of the defunct but legendary Wall Street firm Salomon Brothers, a choice laden with historical irony.[15] The

/owner-notice page hosted a formal legal notice. It claimed "constructive possession" of the dormant wallets and issued a 90-day ultimatum (with a deadline cited as September 30 or October 5, 2025, depending on the report) for the "bona fide owner" to prove their ownership.[1] The site offered two methods for proof: signing an on-chain message with the private key or submitting personal information via a web form—the latter being a classic phishing technique to de-anonymize the owner.[15] This entire framework was an attempt to apply the real-world legal doctrine of "adverse possession," typically used for real estate, to the novel context of digital assets.[1]

Real-World Connections and Misdirection

Adding another layer of intrigue, on-chain researcher @Cyphertux noted that the address listed on the salomonbros.com website corresponded to the physical headquarters of EisnerAmper, a major accounting and advisory firm known for its blockchain investigation and forensic services.[13] EisnerAmper has collaborated with the investigator credited with unmasking Ross Ulbricht, the founder of the Silk Road darknet market.[13] This connection serves a dual purpose: it either suggests an incredibly audacious operation with links to legitimate forensic or legal entities, or it is a masterfully crafted red herring designed to point suspicion toward state-level actors and away from the true perpetrators.

Table 1: On-Chain Transaction Summary

The following table provides a consolidated, authoritative reference for the core on-chain data related to the 80,000 BTC movement, compiled from multiple on-chain analysis reports and blockchain explorers. It serves as the factual foundation for the analysis in this report.

Source Address (P2PKH)	Initial Funding Date(s)	Main BTC TXID (July 4-5, 2025)	Destination Address (SegWit)	Notes
12tLs9c9RsALt4ockxa1hB4iTCTSmxj2me	Apr 2, 2011	9d5d67169a37222720b407c99939f7baa40587eef9ab16ec3a17c7c856ef9045 [19]	Unknown bc1q... address	Confirmed source of the pre-emptive BCH test transaction.[7]
1KbrSKrT3GeEruTuuYYUSQ35JwKbrAWJYm	Apr 2, 2011	6ba8cefee9a922de94d9faa4f65128967ba2b166d0e85eee8a4ace1d045a3b42 [20]	Unknown bc1q... address	Received multiple dust transactions over the years.[21]
1P1iThxBH542Gmk1kZNXyji4E4iwpvSbrt	May 4, 2011	702c8af9e767cbdfb47d4dca3a875f8a890f476f0105e41d582ea3fa904997aa [22]	Unknown bc1q... address	Was a target of the "Lost Numbers" OP_RETURN message.[7]
1CPaziTeda2b4ih295L3s5a4hT4T7yK1eR	May 4, 2011	*TXID Not Found in Sources*	Unknown bc1q... address	Identified as part of the 8-wallet cluster.[7]
14YK4mz... (Partial)	May 4, 2011	*TXID Not Found in Sources*	Unknown bc1q... address	Identified as part of the 8-wallet cluster.[7]
1ucXXZQ...	May 4, 2011	*TXID Not Found*	Unknown bc1q...	Identified as

(Partial)		*in Sources*	address	part of the 8-wallet cluster.[7]
1BAFWQhH9pNkz3mZDQ1tWrtKkSHVCkc3fV	May 4, 2011	*TXID Not Found in Sources*	Unknown bc1q... address	Was a target of all four sequential OP_RETURN messages.[7]
1f1miYFQWTzdLiCBxtHHnNiW7WAWPUccr	May 4, 2011	138e8e608fc406baea409e2e52e0edad77104d9b282da4eb6c515386398d45fe [23]	bc1qwq5geath93h0lnfsrmnwnfuck2f9ypv4ewyl4j	Destination is a provocative vanity address.[7]

Section II: The Public Square — A Corpus of Competing Narratives

The July 4th Anomaly triggered a massive, global effort to interpret the on-chain facts. This section deconstructs the public response, categorizing the dominant hypotheses that emerged on platforms like Reddit, Twitter, and the Bitcointalk forum. It analyzes the evidence cited for each theory and provides a sentiment analysis reflecting its prevalence and credibility within different communities. A key finding is the stark gap between how mainstream finance and crypto-native communities interpreted the same set of facts, revealing a fundamental difference in risk perception and analytical frameworks.

2.1 Hypothesis A: The "Panicked Owner"

- **Core Argument:** This hypothesis posits that the events were initiated by the legitimate, original owner of the 80,000 BTC. A long-term holder, this individual was likely spooked by the aggressive OP_RETURN spam and the professional-looking legal threats on the salomonbros.com website. In response, they decided to move their vast fortune from the old, potentially vulnerable P2PKH wallets to more secure, modern SegWit addresses to preemptively protect their assets.[3] The entire operation is thus framed as a prudent, if large, security upgrade.[5]

- **Supporting Evidence:** Proponents of this theory point to several key facts. First, the destination addresses were new SegWit wallets, which is an established best practice for enhancing security and lowering transaction fees.[5] Second, none of the funds were sent to cryptocurrency exchanges, which eases fears of an immediate sale and suggests the motive was consolidation, not liquidation.[5] Finally, the timing of the transfers, occurring shortly after the OP_RETURN messages were broadcast, strongly suggests a direct reaction to the perceived threat.[3]
- **Sentiment:** This explanation was widely reported and favored by mainstream financial news outlets and generalist publications.[3] It is the simplest, least alarming, and most easily digestible narrative, as it does not imply a breach of Bitcoin's security. However, among deep crypto analysts and on-chain forensics communities, it is considered a less likely, though still plausible, theory.[4] The sheer theatricality of the event seems inconsistent with the quiet prudence of a security-conscious owner.

2.2 Hypothesis B: The "Legal Exploit / Sophisticated Heist"

- **Core Argument:** This is the antithesis of the "Panicked Owner" theory. It argues that the transfer was not a defensive move by the owner, but a hostile takeover by a sophisticated attacker who had successfully compromised the private keys through a cryptographic exploit.[2] The elaborate legal facade, the OP_RETURN messages, and the salomonbros.com website were not the cause of the transfer but rather a brilliant and integral part of the attack itself—a smokescreen designed to legitimize the theft, create legal ambiguity, and psychologically manipulate both the victim and the public.[1]
- **Supporting Evidence:** This theory is supported by the technical and operational details of the event. The extreme precision and coordination of the simultaneous moves from eight independent wallets suggest automation and singular control, not a human owner manually managing keys.[2] The use of a Bitcoin Cash test transaction is a key piece of evidence, as it demonstrates a cold, calculated verification of the exploit before the main attack—a step a legitimate owner would have no need to take.[4] Furthermore, the cryptic and taunting nature of the "Lost Numbers" message and the vanity address are seen as the signature of a defiant hacker, not a discreet billionaire.[2] Conor Grogan, Head of Product at Coinbase,

publicly floated this possibility, calling it potentially the "biggest theft in history" if the wallets were indeed compromised.[4]

- **Sentiment:** This is the dominant theory among on-chain analysts, cryptographic researchers, and the crypto-native community.[4] It is viewed as the most compelling explanation because it accounts for the full spectrum of evidence—the technical sophistication, the psychological manipulation, and the legal theater.

2.3 Hypothesis C: The "White Hat / Ethical Warning"

- **Core Argument:** This hypothesis offers a more optimistic interpretation of the hostile takeover theory. It posits that the actor is a "white hat" or "ethical hacker" who independently discovered a critical vulnerability in how early Bitcoin wallets generated their keys. The 80,000 BTC transfer was a massive, public proof-of-concept designed to be so spectacular that it would force the Bitcoin community, developers, and holders of other legacy wallets to acknowledge and address the vulnerability before it could be exploited maliciously by criminals on a wider scale—perhaps even against the wallets of Satoshi Nakamoto himself.[1] Under this theory, the actor has no intention of keeping the funds and may eventually attempt to return them or work with law enforcement to secure them on behalf of the original owner.
- **Supporting Evidence:** The primary evidence for this theory is the actor's post-exploit behavior. They could have immediately laundered and sold the 80,000 BTC but instead chose to move them to new, unspent addresses.[5] The highly public nature of the act, using OP_RETURN messages to announce their presence, can be interpreted as a form of responsible (albeit dramatic) disclosure rather than a stealthy theft.[1] There are historical precedents in the crypto space, particularly on the Ethereum platform, where white hat groups have moved funds from vulnerable smart contracts to safeguard them from impending attacks.[27]
- **Sentiment:** This is a hopeful but less-cited theory. It is popular among those in the community who wish to see a positive, ecosystem-strengthening outcome from the event. However, it is often viewed as less likely due to the aggressive and intimidating legal language used in the OP_RETURN messages and on the website, which seems more aligned with a hostile act than an ethical warning.[28]

2.4 Hypothesis D: The "Craig Wright / Red Herring"

- **Core Argument:** This theory suggests that the event was deliberately seeded with tangential "clues" and stylistic elements that mimic the behavior of controversial figures like Craig Wright, the Australian computer scientist who claims to be Satoshi Nakamoto. The purpose of these clues was not to genuinely point to Wright as the perpetrator, but to act as a sophisticated red herring, designed to sow chaos, misdirection, and endless debate, thereby camouflaging the true identity and methods of the attacker.
- **Supporting Evidence:** On-chain analyst @Cyphertux noted the bizarre coincidence that a PDF document related to Craig Wright was reportedly modified on the same day as the event.[26] Furthermore, Wright has a well-documented history of using legal threats and making claims about "Solomon's" keys, which stylistically mirrors the event's tactics.[29] A sophisticated actor would know that any link, however tenuous, to Wright would instantly trigger a massive and distracting storm of debate, ridicule, and media attention, providing perfect cover for their operation.
- **Counter-Argument:** Craig Wright has repeatedly failed in court and in public to provide any cryptographic proof that he is Satoshi Nakamoto or that he controls any of Satoshi's wallets.[3] His credibility within the technical community is effectively zero. Therefore, the idea that he himself could execute an exploit of this sophistication is widely dismissed.
- **Sentiment:** The theory that Craig Wright was literally behind the event is considered a fringe theory with very low credibility. However, the more nuanced interpretation—that the event was *designed to look like something he would do* as a deliberate misdirection—is seen as highly plausible by sophisticated analysts who appreciate the value of narrative warfare.[26]

2.5 Hypothesis E: The "State-Level Actor"

- **Core Argument:** This hypothesis posits that a government agency, such as the U.S. Internal Revenue Service (IRS) or the Federal Bureau of Investigation (FBI), was behind the operation. The motive could be twofold: either to seize digital assets that are deemed abandoned or illicitly obtained, or to "tag" these high-value, anonymous coins to track their future movement through the global financial system for intelligence and law enforcement purposes.

- **Supporting Evidence:** Government agencies are known to be actively tracking cryptocurrency transactions and employ blockchain analysis firms like Chainalysis to do so.[32] The highly organized, well-resourced, and methodical nature of the operation is consistent with the capabilities of a state actor. The legalistic language of the
OP_RETURN notices and the salomonbros.com website, which attempts to establish a claim on "abandoned" property, closely mimics the legal processes of civil forfeiture or seizure.[1] The most compelling piece of circumstantial evidence is the link to EisnerAmper, a real-world forensic accounting firm with a history of involvement in major federal cases.[13]
- **Sentiment:** This is a speculative but persistent theory, particularly popular among those with a cypherpunk or anti-government worldview. While difficult to prove without a direct admission, it fits the profile of the operation's sophistication and its blending of technical and legal tactics.

The most credible of these hypotheses—the Heist, the White Hat, and the State Actor—all converge on a single, vital prerequisite: a successful cryptographic exploit. The variations are about the *motive* and *identity* of the actor, not the fundamental *method*. This establishes that the core of the investigation must be the technical vulnerability that allowed the private keys to be compromised in the first place. The rest, from the legal threats to the cryptic numbers, is theater built around this central technical achievement. This event also pioneers a new form of hybrid attack that could be termed "Legal-Ware": the use of legal concepts and threats as an active component of a digital asset exploit, designed to paralyze the victim with uncertainty while the technical attack secures the assets.

Section III: The Ghost in the Machine — A Technical Deep Dive into the Exploit

To understand how 80,000 BTC could be moved from wallets untouched for 14 years, it is essential to analyze the technical underpinnings of the most credible hypothesis: a cryptographic exploit targeting weaknesses in early Bitcoin wallets. This section provides a detailed analysis of the vulnerabilities in legacy address formats and the sophisticated attack methods used to compromise them, presented in a manner accessible to a non-cryptographic expert. The core of the issue is not a flaw in the Bitcoin protocol itself, but rather in the historical implementation of the software used to generate the keys.

3.1 Bitcoin's Cryptographic Lineage: P2PKH's Faded Glory

The wallets targeted in the July 4th event were all of the Pay-to-PubKey-Hash (P2PKH) type, the original and oldest address format in Bitcoin.[7] Understanding the differences between this legacy format and modern standards is crucial to grasping why these specific wallets were vulnerable.

- **P2PKH (Legacy):** These addresses, which start with the number '1', were the standard in Bitcoin's early years (2009-2013).[9] In a P2PKH scheme, the public address is a hash of the owner's public key. The full public key itself is not revealed on the blockchain until the *first time* funds are spent from that address.[35] While this provides a layer of protection against attacks that require the full public key (like quantum attacks), the primary vulnerability of these addresses lies in how their corresponding private keys were generated. Early wallet software and websites from that era often used flawed or weak Random Number Generators (RNGs), which could lead to predictable or biased private keys.[2] P2PKH addresses are also less efficient, resulting in higher transaction fees compared to modern formats.[9]
- **SegWit (P2WPKH):** Introduced in 2017, Segregated Witness (SegWit) was a major network upgrade designed to improve scalability and fix transaction malleability. Native SegWit addresses (P2WPKH) begin with 'bc1q'.[9] By separating the digital signature data (the "witness") from the core transaction data, SegWit allows more transactions to fit into a block, thus lowering fees.[10] From a security perspective, SegWit wallets are generated by modern software with more robust standards for randomness, and the address format itself includes better error-correcting codes to prevent typos.[9]
- **Taproot (P2TR):** The most recent major upgrade, activated in 2021, introduced Taproot addresses, which begin with 'bc1p'.[9] Taproot brings significant enhancements to privacy and smart contract capabilities, primarily through the implementation of Schnorr signatures. Schnorr signatures allow for signature aggregation, which makes complex multi-signature transactions (common for high-security institutional custody) appear indistinguishable from simple, single-signature transactions on the blockchain.[38] From a security standpoint,

Taproot is a major leap forward. It can be structured to *never* reveal the full public key on-chain, even after funds are spent, offering a powerful theoretical defense against a future class of quantum computing attacks that could derive a private key from its corresponding public key.[11]

Table 2: Comparative Analysis of Bitcoin Address Formats

This table visually articulates the evolution of Bitcoin addresses and highlights why the 2010-2011 P2PKH wallets were a specific and viable target for the July 4th exploit. It frames the event not as a failure of "Bitcoin" as a whole, but as the exploitation of a specific, legacy component of the system.

Feature	P2PKH (Legacy, c. 2011)	SegWit (P2WPKH, c. 2017)	Taproot (P2TR, c. 2021)
Address Prefix	1...	bc1q...	bc1p...
Signature Algorithm	ECDSA	ECDSA	Schnorr Signatures
Public Key Exposure	Exposed on first spend [35]	Exposed on first spend	Can be structured to never expose [36]
Primary Vulnerability	**Weak RNG in early wallet software leading to biased ECDSA nonces** [2]	Transaction Malleability (largely fixed)	Theoretical attacks; more robust design
Quantum Resistance	Low (if pubkey is exposed)	Low (if pubkey is exposed)	Higher (due to Schnorr/MAST privacy) [11]
Privacy	Low	Medium	High [10]
Fee Efficiency	Low [9]	High	Highest (for complex transactions) [10]

3.2 The Achilles' Heel of ECDSA: The Nonce

The cryptographic exploit at the heart of the July 4th Anomaly targets a subtle but critical component of the Elliptic Curve Digital Signature Algorithm (ECDSA), the system Bitcoin uses to verify transactions.[41]

- **The Critical Nonce (k):** To create a digital signature, the ECDSA algorithm requires the signer's private key, the hash of the message being signed, and a secret, single-use random number known as a "nonce," denoted by the variable k.[40] The security of the entire system hinges on this nonce being unpredictable and unique for every single signature created with the same private key.
- **Nonce Reuse Catastrophe:** If the *exact same* nonce k is ever used to sign two different messages with the same private key, the private key is no longer secret. It can be trivially recovered using simple algebra from the two public signatures.[40] This is not a theoretical flaw; it is a well-known implementation bug that was responsible for the infamous 2010 Sony PlayStation 3 hack, where Sony used a static, non-random nonce, allowing hackers to calculate the console's master signing key.[40]
- **Biased Nonce Vulnerability:** The July 4th event likely did not involve such a blatant reuse of the exact same nonce. The attack was more sophisticated, exploiting a more subtle but equally devastating flaw: **biased nonces**. If the Random Number Generator (RNG) used by the wallet software to create the nonce k is flawed, the nonces it produces are not truly random. They may exhibit predictable patterns. For example, they might be consistently shorter than the required 256 bits, or a certain number of their leading bits might always be zero.[26] This was precisely the vulnerability that led to the theft of funds from some Android Bitcoin wallets in 2013, which used a flawed implementation of Java's SecureRandom class.[40] The wallets targeted on July 4th, created in the 2010-2011 era, are from a period notorious for such weak RNG implementations in early Bitcoin software.[7]

3.3 The Art of the Lattice Attack: Breaking Biased Signatures

When a private key has been used to create multiple signatures with biased nonces, it becomes vulnerable to a powerful cryptanalytic technique known as a lattice attack.[47]

- **The Concept:** A lattice attack can recover a secret private key by analyzing a collection of public signatures that were all created using nonces from a weak or biased RNG. It does not require knowing the nonces, only that they share a predictable flaw.

- **The Mechanics (Simplified):**
    1. **The Hidden Number Problem (HNP):** The core mathematical challenge is known as the Hidden Number Problem. Each biased signature provides a small, imperfect "clue" about the secret private key. The HNP is the problem of finding the full secret number (the private key) when all you have is a large collection of these fuzzy clues.[42] The ECDSA signature equation, $s=k-1(h+dr)(modn)$, can be rearranged to $k \equiv s-1h+(s-1r)d(modn)$. If the nonce k is biased (e.g., small), this equation provides a linear congruence that gives a hint about the private key d.
    2. **Lattices as a Geometric Tool:** The attacker takes these mathematical clues (the linear congruences from each signature) and represents them as a set of vectors in a high-dimensional space. These vectors define the points of a geometric grid-like structure called a lattice.[52]
    3. **Finding the Shortest Vector:** The solution to the system of equations—which reveals the private key—corresponds to a uniquely "short" vector (or a path between two points) within this highly complex lattice. The problem of finding the private key is thus transformed into a geometric problem of finding the shortest path in the lattice.
    4. **Lattice Reduction Algorithms (LLL/BKZ):** While finding the absolute shortest vector in a lattice is computationally hard, powerful algorithms like LLL (Lenstra-Lenstra-Lovász) and BKZ (Block Korkine-Zolotarev) can efficiently find a very short vector that is often the correct solution.[43] By feeding the public signature data into these algorithms, an attacker can solve the HNP and recover the private key. The attack's success rate increases with the number of signatures collected and the degree of bias in the nonces.[42]

3.4 Case Study: The "JohnnyTX" / Puzzle #130 Precedent (July-September 2024)

The feasibility of such an attack is not merely theoretical. The events of July-September 2024 provided a stunning public demonstration of the resources and techniques required.

- **The Puzzles:** The Bitcoin "Transaction Puzzles," created by a user named "JohnnyTX" and others, are a long-standing challenge in the community. They consist of Bitcoin addresses funded with real BTC, but with private keys that are intentionally weakened. For example, a key might be a 256-bit number where the first 190 bits are all zero, leaving only 66 bits of "entropy" to be discovered.[55]

- **The 2024 Breakthroughs:** In the summer of 2024, the community witnessed the solving of several high-difficulty puzzles that had been outstanding for years. Notably, Puzzle #66 (with 66 bits of entropy) was solved, and even more significantly, Puzzle #130 was cracked.[55] Puzzle #130 was a special case where the public key was known, reducing the effective work to break the 130-bit key to roughly
  265 operations using algorithms like Pollard's rho.[55]
- **Significance as a Precursor:** The solving of these puzzles was a critical technical precursor to the July 4th Anomaly. It served as a public, real-world benchmark, proving that the computational power (via massive, distributed GPU clusters) and the mathematical algorithms needed to break keys with a known degree of weakness were now practically accessible to well-resourced, non-state actors. For a sophisticated attacker planning the 80k BTC heist, the fall of Puzzle #130 was the "canary in the coal mine"—a clear signal that their planned attack against real-world wallets with similar (or greater) weaknesses from the weak RNG era was now computationally feasible.

The convergence of these factors—the existence of a pool of legacy P2PKH wallets created with flawed software, the public nature of the blockchain allowing for the collection of signatures over many years, and the recent democratization of the computational power and algorithms needed to execute a lattice attack—created the perfect storm for the July 4th Anomaly.

Section IV: The Aftershock — Systemic Risks and the Future of Bitcoin

The July 4th Anomaly transcends a mere transfer of funds; it is a seismic event that exposes fundamental challenges and systemic risks within the Bitcoin ecosystem. Its aftershocks will reverberate for years, impacting the network's technical evolution, its economic narratives, its legal standing, and its appeal to institutional investors. The event forces a confrontation with difficult questions about Bitcoin's ability to adapt, the certainty of its supply, the nature of digital ownership, and the fragility of its market narrative.

4.1 Cryptographic Agility: Bitcoin's Inability to Evolve

The exploit of legacy P2PKH wallets serves as a stark and practical illustration of "cryptographic obsolescence"—the inevitable process by which cryptographic algorithms are weakened over time by advances in computing and cryptanalysis.[59] The July 4th event is a live-fire drill for the much larger, long-anticipated threat of quantum computing, which is expected to one day break the ECDSA algorithm entirely.[24]

This highlights a core structural challenge for Bitcoin: its lack of cryptographic agility. Crypto-agility is the ability of a system to seamlessly transition to new, stronger cryptographic algorithms without disruptive changes to its infrastructure.[60] For a centralized service, such an upgrade can be mandated from the top down. For a decentralized network like Bitcoin, it is a monumental undertaking that requires broad, voluntary consensus among thousands of independent miners, developers, and users to implement a network-wide soft or hard fork.

The slow adoption of past upgrades like SegWit and Taproot demonstrates this inertia. While Taproot offers superior security and privacy, a significant portion of the network continues to use older, less secure address formats.[39] The July 4th Anomaly proves that this is not a theoretical risk. The inability to easily and swiftly migrate the entire network to state-of-the-art cryptographic standards represents a profound systemic vulnerability. The network's strength—its decentralized and consensus-driven nature—becomes a weakness when rapid evolution is required to counter an emerging threat.

4.2 Supply Uncertainty: The Myth of the Lost Coins

A cornerstone of Bitcoin's economic narrative and valuation models is its absolute, predictable scarcity, capped at 21 million coins. Embedded within this narrative is the widespread assumption that a significant portion of the "ancient supply"—coins that have not moved in over a decade—is permanently lost and thus removed from circulation.[62] As of June 2025, this ancient supply accounted for over 17% of all issued

Bitcoin, or nearly 3.4 million BTC.[63]

The July 4th Anomaly shatters this comforting myth. The sudden re-entry of 80,000 coins, previously presumed dormant or lost, into the active supply constitutes a significant supply shock.[5] It forces a radical re-evaluation of a critical question: how much Bitcoin is truly lost, and how much is merely dormant and potentially recoverable by a sophisticated actor?

If the cryptographic weaknesses that enabled this event are present in other large, dormant wallets from the same era—including, hypothetically, the million-coin stash attributed to Satoshi Nakamoto—the effective circulating supply of Bitcoin could be substantially larger than current models assume. This introduces a new, unquantifiable variable into Bitcoin's supply dynamics. The potential for other "ghost" wallets to reawaken could create long-term downward pressure on price, challenging the core "digital scarcity" narrative that underpins much of its value proposition and institutional appeal.[62]

4.3 Legal & Ownership Void: "Code is Law" vs. Property Law

The actor's methodical use of the salomonbros.com website and the legalistic OP_RETURN messages was not merely theater; it was a calculated legal gambit designed to force a confrontation between two fundamentally different concepts of ownership.

- **The "Code is Law" Ethos:** Within the native crypto ecosystem, the prevailing ethos is that "code is law." Possession of the private key is absolute proof of ownership, granting the holder the sole and irrevocable right to control the associated assets.[15] In this world, the actor who successfully compromised the keys is the new, legitimate owner.
- **Traditional Property Law:** In the traditional legal world, ownership is a bundle of rights granted and protected by the state. Concepts like "abandoned property" and "adverse possession" provide legal frameworks through which ownership can be transferred even without the original owner's consent, provided certain conditions are met.[66]

The July 4th Anomaly deliberately crashes these two worlds into each other. The actor created a public, immutable record of their "claim" on what they framed as "abandoned" property, and they provided a "remedy" period for the original owner to come forward.[1] This raises a novel and deeply disruptive legal question: If an asset has been digitally "abandoned" on-chain for 14 years, can a third party use a cryptographic exploit to take control of it and then seek protection and legitimacy under the framework of traditional property law? This event opens a Pandora's box of legal ambiguity, creating a void that courts and regulators will be forced to address.

4.4 Narrative Fragility: A Blow to Institutional Confidence

For the nascent institutional adoption of Bitcoin, the July 4th Anomaly is a devastating blow. The nuanced technical reality—that a specific, legacy component was exploited—is often lost in the broader market. The headline risk of "80,000 BTC Stolen" or "Bitcoin Hacked" is profoundly damaging to market confidence.[68]

Institutional investors, such as pension funds, endowments, and large corporations, require predictability, robust security, and clear legal recourse before deploying capital at scale.[68] This single event undermines all three pillars of institutional confidence:

- **Security:** It introduces a new, highly technical, and difficult-to-understand security risk (lattice attacks on legacy wallets) that was previously considered largely theoretical.
- **Predictability:** It creates fundamental uncertainty about the true circulating supply of Bitcoin, disrupting the scarcity models upon which institutional theses are built.
- **Legal Recourse:** It highlights a legal and ownership void, demonstrating that even a multi-billion dollar fortune can be compromised with unclear paths to recovery or justice.

This could cause risk-averse institutions to pause, reverse, or delay their adoption of Bitcoin, fearing not only direct financial loss but also significant reputational damage and regulatory scrutiny.[69] The fact that major investment products like spot Bitcoin ETFs rely on single custodians like Coinbase further concentrates this risk, creating a potential single point of failure that is antithetical to Bitcoin's decentralized ethos.[70]

The aftermath of this event will serve as a critical test of Bitcoin's decentralized governance. There will inevitably be calls for radical, centralized solutions, such as a hard fork to reverse the transactions—a move that would violate the core principle of immutability. Conversely, a "do nothing" approach would uphold the "code is law" ethos but would effectively ratify an $8.6 billion theft. The ensuing debate will reveal the true political and philosophical fault lines within the Bitcoin community and set a powerful precedent for how the network confronts future existential threats.

Conclusion: A Paradigm Shift in Digital Risk

The July 4th Anomaly, irrespective of the actor's ultimate identity or motive, represents a fundamental and irreversible turning point for Bitcoin and the broader digital asset space. It marks the moment when a long-theorized class of sophisticated cryptographic attacks transitioned from the academic to the practical, executed at a scale previously unimaginable. The event was not a simple hack but a masterfully orchestrated operation, blending high-level cryptanalysis with legal maneuvering and psychological warfare.

This report's analysis leads to several key conclusions. First, the weight of the on-chain evidence overwhelmingly supports the hypothesis of a hostile takeover via a cryptographic exploit, rendering the "panicked owner" narrative untenable. The methodical precision, the cross-chain "canary" test, and the elaborate narrative construction are the hallmarks of a professional adversary.

Second, the event shatters the comforting illusion of "lost coins," which has long been a quiet pillar of Bitcoin's scarcity narrative. The sudden reanimation of 80,000 BTC forces a market-wide repricing of risk associated with the vast trove of dormant, legacy-era wallets. This introduces a new and significant element of supply uncertainty that could have lasting economic consequences.

Third, the incident exposes the critical challenge of "cryptographic agility" for decentralized networks. Bitcoin's resistance to change, a feature that provides stability, becomes a liability when its underlying cryptography is threatened by obsolescence. The July 4th Anomaly is a stark warning that the network must find ways to evolve more rapidly to counter future threats, most notably the advent of quantum computing.

Finally, the event ignites a crucial and unavoidable conflict between the nascent, code-based laws of the blockchain and the established property laws of the traditional world. The actor's legal gambit forces a societal and judicial reckoning with the question of what constitutes ownership and abandonment in the digital realm.

The July 4th Anomaly is, in essence, a forced maturation of the ecosystem. It demands a more nuanced and sophisticated understanding of risk, where not all bitcoins are considered equal. It will likely catalyze the creation of a new risk classification—"Cryptographically Vulnerable Property"—and accelerate the migration away from legacy systems. While profoundly disruptive, the attack may inadvertently serve as the most powerful catalyst for a network-wide security upgrade in Bitcoin's history. It is a painful but necessary lesson, demonstrating that in a world built on pure mathematics, the elegance of an algorithm can be as powerful as any army, capable of summoning or seizing fortunes and reshaping the future of finance.

Alıntılanan çalışmalar

1. Whale Moves 80,000 Bitcoin Worth $8.6 Billion to New Addresses, erişim tarihi Temmuz 12, 2025, https://www.ainvest.com/news/whale-moves-80-000-bitcoin-worth-8-6-billion-addresses-2507/
2. Who Cracked Bitcoin on July 4th? 80000 BTC Moved in What Might Be the First Real Exploit — and You Missed it. | by Eloise | Jul, 2025, erişim tarihi Temmuz 12, 2025, https://eloise88.medium.com/who-cracked-bitcoin-on-july-4th-408230a70f5d
3. The world's greatest mystery: Who is Satoshi Nakamoto and how rich is Bitcoin's elusive creator? - The Economic Times, erişim tarihi Temmuz 12, 2025, https://m.economictimes.com/news/international/us/the-worlds-greatest-mystery-who-is-satoshi-nakamoto-and-how-rich-is-bitcoins-elusive-creator/articleshow/122381331.cms
4. 80000 BTC Moved After 14 Years: Mystery Transfer or Massive Hack? - TradingView, erişim tarihi Temmuz 12, 2025, https://www.tradingview.com/news/coinpedia:21d711485094b:0-80-000-btc-moved-after-14-years-mystery-transfer-or-massive-hack/
5. Bitcoin starts week near record high as 80K BTC moves after 14 ..., erişim tarihi Temmuz 12, 2025, https://blockworks.co/news/satoshi-era-wallets-transfer-btc
6. Mysterious $8 Billion Bitcoin Move: Quantum Theft, Legal Seizure, or Hoax? - YouTube, erişim tarihi Temmuz 12, 2025, https://www.youtube.com/watch?v=9UvrxvXz17w
7. 80,000 BTC Moved: A Turning Point in Bitcoin History, erişim tarihi Temmuz 12, 2025, https://www.cyphertux.net/articles/en/research/bitcoin-80k-btc-mystere-opretur n
8. Largest-ever transaction of $8.6B of Satoshi-era bitcoins, held in custody for more than 14 years and bought at rock-bottom prices - AS USA, erişim tarihi Temmuz 12, 2025, https://en.as.com/latest_news/largest-ever-transaction-of-86b-of-satoshi-era-bi

tcoins-held-in-custody-for-more-than-14-years-and-bought-at-rock-bottom-prices-n/

9. Address | Bitcoin Design, erişim tarihi Temmuz 12, 2025, https://bitcoin.design/guide/glossary/address/
10. Types of bitcoin addresses: which one to choose in 2025? Legacy, SegWit, Taproot | by AML Crypto | Medium, erişim tarihi Temmuz 12, 2025, https://medium.com/@AMLCrypto/types-of-bitcoin-addresses-which-one-to-choose-in-2025-legacy-segwit-taproot-0138af5610ec
11. Bitcoin Taproot vs Native SegWit: Which Is Better for You? - Komodo Platform, erişim tarihi Temmuz 12, 2025, https://komodoplatform.com/en/academy/bitcoin-native-segwit-vs-taproot/
12. Best Crypto to Buy Now as $8.6B Bitcoin Whale Awakens After 14 Years - Cryptodnes.bg, erişim tarihi Temmuz 12, 2025, https://cryptodnes.bg/en/best-crypto-to-buy-now-as-8-6b-bitcoin-whale-awakens-after-14-years/
13. 80 000 Bitcoins réveillés : Enquête sur un mystère à 8,6 Milliards de ..., erişim tarihi Temmuz 12, 2025, https://journalducoin.com/bitcoin/80-000-bitcoins-reveilles-enquete-mystere-86-milliards-dollars/
14. 80 000 BTC Mysterium: Rechtliche Ansprüche werfen Fragen auf, erişim tarihi Temmuz 12, 2025, https://www.bitget.com/de/news/detail/12560604858266
15. New Bitcoin Scam Unfolds: Old Wallets, Fake Lawyers - Mitrade, erişim tarihi Temmuz 12, 2025, https://www.mitrade.com/insights/news/live-news/article-3-943804-20250709
16. 8 Largest Lost Bitcoin Wallets Ever - Webopedia, erişim tarihi Temmuz 12, 2025, https://www.webopedia.com/crypto/learn/largest-ost-bitcoin-wallets/
17. Bitcoin Dust: Overview, Disadvantages, and Example - Investopedia, erişim tarihi Temmuz 12, 2025, https://www.investopedia.com/terms/b/bitcoin-dust.asp
18. Societe Nationale D'Exploitation v. Salomon Bros., 928 F. Supp. 398 (S.D.N.Y. 1996), erişim tarihi Temmuz 12, 2025, https://law.justia.com/cases/federal/district-courts/FSupp/928/398/1446819/
19. Transaction | Whale Alert, erişim tarihi Temmuz 12, 2025, https://whale-alert.io/transaction/bitcoin/9d5d67169a37222720b407c99939f7baa40587eef9ab16ec3a17c7c856ef9045
20. Transaction | Whale Alert, erişim tarihi Temmuz 12, 2025, https://whale-alert.io/transaction/bitcoin/6ba8cefee9a922de94d9faa4f65128967ba2b166d0e85eee8a4ace1d045a3b42
21. Address: 1KbrSKrT3GeEruTuuYYUSQ35JwKbrAWJYm - mempool - Bitcoin Explorer, erişim tarihi Temmuz 12, 2025, https://mempool.space/address/1KbrSKrT3GeEruTuuYYUSQ35JwKbrAWJYm
22. Transaction | Whale Alert, erişim tarihi Temmuz 12, 2025, https://whale-alert.io/transaction/bitcoin/702c8af9e767cbdfb47d4dca3a875f8a890f476f0105e41d582ea3fa904997aa
23. Transaction | Whale Alert, erişim tarihi Temmuz 12, 2025, https://whale-alert.io/transaction/bitcoin/138e8e608fc406baea409e2e52e0edad

77104d9b282da4eb6c515386398d45fe

24. Did Quantum Fears Prompt a Bitcoin Whale to Make an $8 Billion Move?, erişim tarihi Temmuz 12, 2025, https://thequantuminsider.com/2025/07/08/did-quantum-fears-prompt-a-bitcoin-whale-to-make-an-8-billion-move/
25. Someone is moving $8B worth of BTC or I don't understand anything? : r/CryptoCurrency, erişim tarihi Temmuz 12, 2025, https://www.reddit.com/r/CryptoCurrency/comments/1lrl70b/someone_is_moving_8b_worth_of_btc_or_i_dont/
26. ECDSA Nonces, Lattice, RNG et Patterns : Decrypting a Bitcoin Exploit - CypherTux OS, erişim tarihi Temmuz 12, 2025, https://www.cyphertux.net/articles/en/research/ecdsa-nonces-lattice-attacks-bitcoin-exploit
27. Signature redacte - DSpace@MIT, erişim tarihi Temmuz 12, 2025, https://dspace.mit.edu/bitstream/handle/1721.1/121793/1103445166-MIT.pdf?sequence=1&isAllowed=y
28. Eintragen, Ändern und Schützen der Blockchain-Datenstruktur - haraldpoettinger.com, erişim tarihi Temmuz 12, 2025, https://haraldpoettinger.com/blockchain-datenstruktur-eintrag/
29. If craig wright is satoshi, what's his excuse to not move some btcs from satoshi's wallet? : r/Bitcoin - Reddit, erişim tarihi Temmuz 12, 2025, https://www.reddit.com/r/Bitcoin/comments/1al1vng/if_craig_wright_is_satoshi_whats_his_excuse_to/
30. Echo Chamber: Craig Wright Takes Twitter Account Private to Avoid Dissidents - CCN.com, erişim tarihi Temmuz 12, 2025, https://www.ccn.com/echo-chamber-craig-wright-takes-twitter-account-private-to-avoid-dissidents/
31. delays on FX reforms - European University Institute, erişim tarihi Temmuz 12, 2025, https://www.eui.eu/Documents/Business-Day-20230713.pdf
32. Can the IRS Track Cryptocurrency? Do Exchanges Report? [2025] - Blockpit, erişim tarihi Temmuz 12, 2025, https://www.blockpit.io/en-us/tax-guides/can-the-irs-track-cryptocurrency
33. Can the IRS Track Your Cryptocurrency? - Federal Lawyer, erişim tarihi Temmuz 12, 2025, https://federal-lawyer.com/blockchain/irs-track-cryptocurrency/
34. Can the IRS Track Cryptocurrency? (2025 Update) - CoinLedger, erişim tarihi Temmuz 12, 2025, https://coinledger.io/blog/can-the-irs-track-cryptocurrency
35. Quantum computers and the Bitcoin blockchain - Deloitte, erişim tarihi Temmuz 12, 2025, https://www.deloitte.com/nl/en/services/risk-advisory/perspectives/quantum-computers-and-the-bitcoin-blockchain.html
36. Whats the difference between Satoshi's keys / BTC to newer ones : r/Bitcoin - Reddit, erişim tarihi Temmuz 12, 2025, https://www.reddit.com/r/Bitcoin/comments/1lwfn10/whats_the_difference_between_satoshis_keys_btc_to/
37. How Bitcoin Addresses Work: Taproot, SegWit, Legacy | Tangem Blog, erişim tarihi

Temmuz 12, 2025, https://tangem.com/en/blog/post/bitcoin-address/
38. Distinguishing the Four Types of Bitcoin Addresses, erişim tarihi Temmuz 12, 2025, https://support.token.im/hc/en-us/articles/33990532648345-Distinguishing-the-Four-Types-of-Bitcoin-Addresses
39. Bitcoin Account Types - Trezor, erişim tarihi Temmuz 12, 2025, https://trezor.io/learn/supported-assets/bitcoin/bitcoin-account-types
40. Elliptic Curve Digital Signature Algorithm - Wikipedia, erişim tarihi Temmuz 12, 2025, https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm
41. Critical Risk in ECDSA: Key Recovery Attack - Hacken, erişim tarihi Temmuz 12, 2025, https://hacken.io/insights/ecdsa/
42. Biased Nonce Sense: Lattice Attacks against Weak ECDSA ..., erişim tarihi Temmuz 12, 2025, https://eprint.iacr.org/2019/023.pdf
43. ECDSA Cracking Methods - arXiv, erişim tarihi Temmuz 12, 2025, https://arxiv.org/html/2504.07265v1
44. pcaversaccio/ecdsa-nonce-reuse-attack: This repository implements a Python function that recovers the private key from two different signatures that use the same random nonce during signature generation. - GitHub, erişim tarihi Temmuz 12, 2025, https://github.com/pcaversaccio/ecdsa-nonce-reuse-attack
45. ECDSA Nonce Reuse Attack - NotSoSecure, erişim tarihi Temmuz 12, 2025, https://notsosecure.com/ecdsa-nonce-reuse-attack
46. Bitcoin account hijacking using OSINT techniques - balasys.eu, erişim tarihi Temmuz 12, 2025, https://balasys.eu/blogs/bitcoin-account-hijacking-ecdsa-nonce-break
47. Biased Nonce Sense: Lattice Attacks Against Weak ECDSA Signatures in Cryptocurrencies, erişim tarihi Temmuz 12, 2025, https://www.researchgate.net/publication/336437771_Biased_Nonce_Sense_Lattice_Attacks_Against_Weak_ECDSA_Signatures_in_Cryptocurrencies
48. bitlogik/lattice-attack: Lattice ECDSA attack - GitHub, erişim tarihi Temmuz 12, 2025, https://github.com/bitlogik/lattice-attack
49. Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies - Financial Cryptography and Data Security 2019, erişim tarihi Temmuz 12, 2025, https://fc19.ifca.ai/preproceedings/104-preproceedings.pdf
50. ECDSA: Handle with Care - The Trail of Bits Blog, erişim tarihi Temmuz 12, 2025, https://blog.trailofbits.com/2020/06/11/ecdsa-handle-with-care/
51. Lattice attacks for side-channel analysis - eShard, erişim tarihi Temmuz 12, 2025, https://eshard.com/escoaching/lattice-side-channel
52. One weak transaction in ECDSA on the Bitcoin blockchain and with the help of Lattice Attack we received a Private Key to BTC coins - GitHub, erişim tarihi Temmuz 12, 2025, https://github.com/demining/Lattice-Attack
53. Lattice Attacks on ECDSA - Vac, erişim tarihi Temmuz 12, 2025, https://forum.vac.dev/t/lattice-attacks-on-ecdsa/136
54. Attacking (EC)DSA Given Only an Implicit Hint - SciSpace, erişim tarihi Temmuz 12, 2025, https://scispace.com/pdf/attacking-ec-dsa-given-only-an-implicit-hint-4riagciy69.pdf

55. Discussion thread here: https://bitcointalk.org/index.php?topic=1306983.msg64526... | Hacker News, erişim tarihi Temmuz 12, 2025, https://news.ycombinator.com/item?id=41547443
56. Bitcoin puzzle #66 was solved: 6.6 BTC (~$400k) withdrawn | Hacker News, erişim tarihi Temmuz 12, 2025, https://news.ycombinator.com/item?id=41547395
57. Bitcoin puzzle #130 solved: 13 BTC ($800k) won; 949 BTC ($60M) left to be won | Hacker News, erişim tarihi Temmuz 12, 2025, https://news.ycombinator.com/item?id=41625745
58. The 66-Bit Puzzle has Been Solved! : r/Bitcoin - Reddit, erişim tarihi Temmuz 12, 2025, https://www.reddit.com/r/Bitcoin/comments/1fg1jbe/the_66bit_puzzle_has_been_solved/
59. What Is Cryptographic Agility | How To Get Crypto-Agility - Encryption Consulting, erişim tarihi Temmuz 12, 2025, https://www.encryptionconsulting.com/education-center/what-is-crypto-agility/
60. Cryptographic agility - Wikipedia, erişim tarihi Temmuz 12, 2025, https://en.wikipedia.org/wiki/Cryptographic_agility
61. Crypto Agility | CSRC - NIST Computer Security Resource Center, erişim tarihi Temmuz 12, 2025, https://csrc.nist.gov/projects/crypto-agility
62. 8 Biggest Dormant BTC Wallets 2025 - Webopedia, erişim tarihi Temmuz 12, 2025, https://www.webopedia.com/crypto/learn/dormant-bitcoin-wallets/
63. The Increasing Impact of Bitcoin's Ancient Supply, erişim tarihi Temmuz 12, 2025, https://www.fidelitydigitalassets.com/research-and-insights/increasing-impact-bitcoins-ancient-supply
64. What Happens to Lost Bitcoin? - River, erişim tarihi Temmuz 12, 2025, https://river.com/learn/what-happens-to-lost-bitcoin/
65. 10+ Year Dormant Bitcoin Whales Come to Life in 2024 - Bitquery, erişim tarihi Temmuz 12, 2025, https://bitquery.io/blog/dormant-bitcoin-wallets-reactivated-insights-market-impact
66. Crypto Losses - Faculty - University of Maine School of Law, erişim tarihi Temmuz 12, 2025, https://mainelaw.maine.edu/faculty/crypto-losses/
67. Can Taxpayers Deduct Losses on Abandoned or Worthless Cryptocurrency? - Withum, erişim tarihi Temmuz 12, 2025, https://www.withum.com/resources/can-taxpayers-deduct-losses-on-abandoned-or-worthless-cryptocurrency/
68. Crypto's Institutional Future Could Hinge on Solving Risk Puzzle, erişim tarihi Temmuz 12, 2025, https://www.pymnts.com/cryptocurrency/2025/crypto-institutional-future-could-hinge-solving-risk/
69. Bitcoin ETFs: Are They the Future of Institutional Adoption? - OneSafe Blog, erişim tarihi Temmuz 12, 2025, https://www.onesafe.io/blog/bitcoin-institutional-adoption-finance-transformation
70. The Hidden Risk in Bitcoin's Big Finance Boom - The Global Treasurer, erişim tarihi

Temmuz 12, 2025, https://www.theglobaltreasurer.com/2025/01/21/the-hidden-risk-in-bitcoins-big-finance-boom/

71. The importance of custodians in bitcoin adoption and ownership - KPMG International, erişim tarihi Temmuz 12, 2025, https://kpmg.com/us/en/articles/2024/importance-custodians-bitcoin-adoption-ownership.html