

The State Of Bitcoin: How the Core vs. Knots Debate Could Shape Bitcoin's Technical, Economic, and Regulatory Future

Connor Aherne
The Bitcoin Policy Institute
August, 2026

Executive Summary

On August 8th, 2026, at block 961,632, the Bitcoin network experienced its first contested chain split in nearly a decade. A minority of node operators running a new proposal called BIP-110 began rejecting blocks that did not signal for the proposal, leading to a chain split. The non-signaling chain continued, generating blocks every 10 minutes. In contrast, the BIP-110 chain crawled to a near standstill, and its supporters are now working to relaunch it as a separate network under a new mining algorithm. The source of this chain split, a debate nearly as old as Bitcoin itself, centers on whether Bitcoin software and its users should discourage people from using the blockchain to store non-monetary data. In this latest chapter in the debate, it erupted into common discourse within the Bitcoin community, with individuals declaring their positions by running one of the two popular node software implementations: Bitcoin Core or Bitcoin Knots.

Core, the dominant node software, which is run by approximately 75% of the network, believes that Bitcoin must remain neutral to all transactions that follow Bitcoin's rules. Knots, the less popular implementation that surged from just 2% to nearly 25% of the network after Core's beliefs sparked controversy, holds that Bitcoin's primary function is to be money and that high-volume data storage imposes real and uncompensated costs on node operators, so software defaults should discourage non-monetary use cases. BIP-110 was the attempt to move this discouragement from an individual choice defined by relay policy, the rules that can be bent per node, into consensus, Bitcoin's primary rules that nodes must follow to remain on the same chain. Approximately 98% of the hashrate did not signal for BIP-110, leading to a consensus disparity and a chain split that caused the BIP-110 chain to fall far behind the dominant non-signaling chain.

Bitcoin Core and Bitcoin Knots represent two schools of thought within Bitcoin that disagree on what Bitcoin's primary thesis should be. Core and its supporters seek to prioritize Bitcoin's neutrality. They believe the most valuable feature of Bitcoin is its ability to relay and confirm consensus-valid transaction data regardless of its purpose, making censorship difficult within what they view as the greatest decentralized database ever developed. Knots and its community reject this definition of Bitcoin, calling it misleading to describe Bitcoin as a database and calling its neutrality toward all transactions destructive to the health of the network. They believe

Bitcoin's dominant thesis is to be the best money and to actively discourage other use cases that may exploit Bitcoin's decentralized, censorship-resistant nature.

It is important to recognize that the dispute is not over Bitcoin's use cases in general, but over which tradeoffs, sacrificing neutrality or monetary attributes, best preserve Bitcoin as it evolves. This long-tested debate within Bitcoin was reignited in October 2025 after Core changed the default setting of a relay-policy filter on OP_RETURN, a segment of a Bitcoin transaction that allows non-monetary data to be attached to a Bitcoin transaction in a cleaner, less-destructive way. Before OP_RETURN, data had to be embedded into transactions using methods that would force the data to sit in the UTXO set forever, meaning all nodes forever had to host and track this data even though it would never be spent again, unlike monetary UTXOs, raising computational costs for node operators over time. OP_RETURN fixed this issue, but while the default relay limit remained at 83 bytes, many users who sought to embed arbitrary data wouldn't use it and instead embedded it in transaction data fields, which bloat the UTXO set. To fix this, Core decided to change the default relay limit to the maximum: 100KB. While Core saw this as harm reduction, Knots users called it an attack that sought to normalize non-monetary data in Bitcoin. This led to the development of Bitcoin Improvement Proposal 110 (BIP-110), the Reduced Data Temporary Soft Fork, which would enforce the original 83-byte relay policy across the entire network by moving it to consensus while also limiting additional data fields used to embed non-monetary data.

This leads to the present, where BIP-110's mandatory signaling period started at block height 961,632, immediately resulting in a chain split when BIP-110 nodes rejected mining pool Antpool's non-signaling block, followed by Roughnecks, a small mining group operating through a decentralized mining pool, mining a BIP-110 signaling block approximately 40 minutes later, permanently dividing the chains. Though many on the Knots side still cling to hope, the common sentiment among the community is that this chapter in the arbitrary data debate is over, with BIP-110 failing to gain the hashrate and node dominance it needed to force the network into this user-activated soft fork. But the failure of BIP-110 does not resolve the questions that created it. The dispute over arbitrary data, and the legal, technical, and philosophical risks it poses to Bitcoin, will remain contentious long after this chain split falls into Bitcoin history. This debate has reached its conclusion at an unusually consequential time for Bitcoin. A volatile market is attempting to value the asset through an unconventional bear market while the Senate is deliberating the Clarity Act, and with it, the regulatory framework through which the United States will define Bitcoin in law. Most recently, the Coldcard hardware wallet hack has forced the community to redefine self-custody, one of the foundational principles of the Bitcoin ethos.

These events, while appearing separate, each test a different characteristic of the same decentralized system. These events raise questions about who determines Bitcoin's rules, how the world will value decentralized permissionless money, and how the state ultimately

understands and assigns responsibility for the infrastructure that makes it all possible. The consequences of this uncertain time, and what Bitcoiners, investors, and policymakers choose to learn from it, will reach far beyond this Core vs. Knots dispute. It will shape Bitcoin across three defining dimensions: Node, price, and state.

This research closes with three recommendations for policymakers, each of which holds regardless of which side of the debate the community settles on. First, protect neutral Bitcoin node operators from liability for third-party misuse, since an operator relays and verifies data they never choose, inspect, or curate. Second, target the individuals intentionally embedding illicit material and use the open ledger to track and potentially apprehend them, rather than the software and the operators that unknowingly relay it. Third, avoid policies that could criminalize decentralized infrastructure. Each is expanded upon in Section VII.

I. Introduction and Methodology

This research began as a deep dive into Bitcoin's arbitrary data debate and its complex history. Throughout the summer of 2026, the outcome of BIP-110, the proposed soft fork attempting to limit data fields used for arbitrary data, was genuinely unknown to both sides. While the fork itself was controversial on its own, a large number of the debates within the community centered on purely the technical outcome of a user-activated soft fork (UASF) and its ability to steer the network with a minority influence, which had never stood on its own before, including in the 2017 Blocksize Wars. To explore this uncharted territory within Bitcoin and make sense of this contention and what was to come of the fork, research was conducted in phases centered around interviews with passionate and technical individuals on both sides. Target individuals to connect with and interview were selected on both sides during independent research. These interviews were conducted primarily over online video calls. Core and Knots supporters were faced with challenging questions on defining arbitrary data and explaining their beliefs on its compatibility with Bitcoin, which then led to a series of critical questions and statements from their opposition, seeking to fully define the limits of both philosophies. Rather than attempting to crown a "correct" implementation, this paper sought to weigh both Core and Knots against identical guidelines: technical effectiveness, economic implications, decentralization goals, node accessibility, censorship resistance, governance implications, and regulatory impact.

Every interview was connected to those preceding and following it, allowing each side to be confronted directly and professionally with the opposing side's strongest arguments and rebuttals. This approach ensured that the positions reproduced in this paper were stress-tested against informed criticism rather than merely stated in isolation. The timing of the research also provided a unique opportunity to observe the final weeks of the debate as BIP-110's mandatory signaling period approached. Uncertainty surrounding the fork's fate, combined with the broader philosophical and technical dispute over BIP-110's legitimacy within Bitcoin, produced an unusually active period of discussion. Participants across the ecosystem contributed arguments,

technical analyses, commentary, and data from competing perspectives, creating a rich body of material for this research despite the considerable noise surrounding the debate. It is important, however, to recognize the limitations of this methodology. The interviews represent a small, selected sample of technically knowledgeable participants in the Core vs. Knots arbitrary-data debate, and the research documents a rapidly evolving event. For this reason, all time-sensitive chain data is identified by block height rather than date alone, and readers are encouraged to verify data with contemporary information, especially as this new fork of Bitcoin's blockchain progresses. Furthermore, blockchain measurements and signaling percentages reported in this research not connected to an external source were independently derived and verified using a full Bitcoin node and on-chain data at the relevant block heights.

This dispute between Bitcoin Core and Bitcoin Knots looks like exactly what its participants often insist it is: a technical argument. Digging deeper, however, reveals that this debate attempts to resolve a complex underlying question: what is Bitcoin's primary identity? Is it a neutral settlement system that must never judge a valid transaction by its purpose, or is it purely decentralized money that must be defended as such to remain successful? This paper argues that the great divide in the Core vs. Knots debate represents a philosophical wedge in technical priorities. The reality is that both sides want the same Bitcoin in nearly every measurable way. Both want decentralized, censorship-resistant, and verifiable money accessible to anyone with modest hardware and the will to participate, but they greatly disagree on which components of Bitcoin require protection and which can be sacrificed for the greater good of the Bitcoin ecosystem. This debate and its consequences will undoubtedly shape Bitcoin's dominant thesis for years to come and radiate outward across three defining fronts: the technical front of the node, where it will determine what it costs an ordinary person to verify their own money; the market front of the price, where it will shape the narrative investors use to value Bitcoin in an unconventional bear market; and the regulatory front of the state, where it may define how policymakers understand and classify this decentralized infrastructure.

II. Technical Foundations

The technical proxies of this debate must be understood before the philosophical divide can be measured and judged accordingly. A disagreement over data limits in a transaction on its own does not seem capable of splitting a network in two, and grasping why requires understanding the following: what a node does, how a transaction is structured, why some forms of data are more expensive to the network than others, and what a user-activated soft fork attempts to accomplish.

The Cost of a Node

A Bitcoin node downloads the history of the entire blockchain and independently verifies every single transaction to confirm it follows Bitcoin's rules. This is a requirement to properly join the

network and run a fully functional node. While running a pruned node, which shortens the stored blockchain to only recent blocks, can help for machines with low disk space, the computation of verifying transactions is still a requirement, and both the computing and storage costs remain as filters that an aspiring node operator must pass to become a sovereign citizen of the Bitcoin blockchain. Operating a personal node is what separates Bitcoin from all other payment networks that require a middleman or administrator, so keeping them easy to create and maintain is crucial to Bitcoin's success.

Consensus and Policy

As the rules of the blockchain, consensus defines what is valid on every node that every participant must follow without exception. A block produced by a node that violates consensus is rejected by the entire network. For example, the twenty-one million coin supply cap in Bitcoin is a consensus rule, and changing it would require overwhelming approval across the network, or the outnumbered few must fork off into their own version of the chain to make their changes. Policy rules define what an individual node operator can choose to accept and relay to its neighboring nodes. An individual node can refuse any transaction it wants, including consensus-valid ones. One of the great attributes of Bitcoin is the reality that a node will eventually relay any transaction, even one shunned by the majority of the network, to a miner that will successfully find a block and cement it in the chain forever. All the individual nodes have done in this scenario is decline to help it travel through the network. One of the primary topics of the Core vs. Knots debate concerns consensus and relay policy. One of BIP-110's goals is to move original relay limits into consensus, forcing the entire network to follow and enforce rules that were previously just discouraged by default policy. This change would reverse Bitcoin Core's decision to change default OP_RETURN relay limits from 83 bytes to the consensus limit, 100 kilobytes. This change was the primary action that sparked the creation of BIP-110 and demonstrates why understanding the intersection of consensus and policy is critical in evaluating both sides of the arbitrary data debate.

Where Non-Monetary Data Gets Into the Blockchain

Put simply, a Bitcoin transaction is built from inputs and outputs. The inputs come from previous outputs from other transactions that have not yet been spent. The collection of every unspent output across the network is called the unspent transaction output (UTXO) set. In a new transaction, these UTXO inputs carry the proof that the spender is the rightful owner of the coins and therefore entitled to spend them, and a separate field called the witness data. The outputs of this transaction become the new spendable coins and join the UTXO set, while the inputs it consumed leave it. Every node must hold the entire current set at all times in order to check whether a new transaction is spending coins that actually exist.

This structure is exactly why different data fields have a different effect on nodes and the network. Old block data can be discarded by a pruned node once it has been verified, but the

UTXO set cannot be discarded by any active node. A byte written into a seemingly spendable output becomes a permanent tax on every node operator who will ever join the network, while a byte written into OP_RETURN is a one-time cost paid during download and verification. Data can be written into a multitude of locations, all with varying degrees of node and operator cost.

Location	What it is	What it costs the network
Fake public key inside an output	Arbitrary data written where a spending condition belongs. Nodes cannot tell it apart from a legitimate address; this spam avenue will remain open.	Worst severity: The output looks spendable and is rarely spent, so it sits in the UTXO set indefinitely and is carried by every node forever.
Witness data	Data written into the section of an input that carries signatures and script material. Inscriptions use this route, and Taproot made it substantially cheaper to use.	Medium severity: It enlarges the blockchain and slows the download and verification of a new node, but it is consumed when spent and never enters the UTXO set.
OP_RETURN output	An output marked unspendable by the OP_RETURN opcode, which causes any attempt to spend it to fail immediately.	Best case scenario: Because it can never be spent, nodes record that it existed and discard it rather than tracking it. It costs blockchain space and adds nothing to the UTXO set.
Satoshi-level fragmentation	Not data storage in itself. The Ordinals numbering scheme identifies individual satoshis, so holders who want to trade them separately must split their holdings into many tiny outputs.	High severity: Each fragment is a genuine spendable output entering the UTXO set, bloating it. Though this is a consequence of the numbering scheme rather than of the data itself.

Origin of OP_RETURN

In early versions of Bitcoin, OP_RETURN was used to end a transaction's script early, and the outputs that utilized it still had to be tracked in the UTXO set. It was then redefined so that any attempt to spend an output containing it failed. This was done to allow nodes to stop tracking those outputs entirely, lessening node burden. For that reason, OP_RETURN can be seen as a settlement rather than a Bitcoin feature. It conceded that users who wanted to embed data would find a way to do it, and OP_RETURN offered them a location that imposed the smallest cost on the network, which was initially fenced in by a small default relay limit to discourage heavy use. In October 2025, over a decade after it was implemented, that default limit was changed in Bitcoin Core Version 30, reigniting the debate on arbitrary data in Bitcoin and what can and should be done about it.

Taproot and Inscriptions

The change to OP_RETURN's default limit was a move toward harm reduction in response to an unhealthy exploit in Bitcoin's transaction structure. Taproot activated in November 2021 at

block height 709,632 with over 90% of miner support. This led to an unanticipated consequence: the witness field, which carries signatures and script material, could now hold large amounts of arbitrary data without adding much to transaction fees. This method for non-monetary data became known as an inscription and was labeled by many as a bug and abuse of Bitcoin's code. This route bypasses OP_RETURN's default limit, so ironically, the relay limit meant to discourage heavy data use was instead encouraging users to use exploits detrimental to the health of the blockchain when they wanted to embed large amounts of arbitrary data. This follows Core's reasoning for the relay limit change in October 2025: if the OP_RETURN limit was no longer discouraging heavy use, then lifting it would invite arbitrary data back into OP_RETURN rather than into more destructive avenues.

Forks, Chain Splits, and UASF

A soft fork tightens the rules of the network, so blocks valid under new rules remain valid under old ones and nodes that didn't upgrade continue to accept the same chain. A hard fork, on the other hand, changes the rules in a way that old nodes reject. This forces every participant to upgrade or be left behind. BIP-110 was designed and advertised as a soft fork, but this did not follow what occurred on August 8th, 2026, which was instead a complete chain split. Soft forks are designed to be resistant to chain splits, but that assurance depends on the majority of mining power enforcing new rules. A user-activated soft fork (UASF) flips this power dynamic by committing in advance to enforce new rules and rejecting blocks that fail to signal when the time comes. In theory, any rational miner would comply rather than risk mining a block that could get rejected. A user-activated soft fork is a coordinated threat of technical enforcement from nodes, but its influence depends on whether that threat is deemed notable by large mining entities. This is where BIP-110 became unique when compared to the previous UASF BIP-148. Deployed during the Blocksize Wars of 2017, it was a soft fork that pressured miners into activating SegWit and succeeded in doing so partly because the economic majority of the network ended up backing it. The question of whether a UASF could work without the same level of consensus, however, was uncharted territory.

BIP-110

BIP-110, known as the Reduced Data Temporary Soft Fork, is a UASF created by a developer under the pseudonym Dathon Ohm. Rather than defining arbitrary data by intent, BIP-110 aimed to reduce and set structural size limits on certain transaction data fields, including restoring the original 83-byte OP_RETURN policy limit as a consensus rule. By limiting scriptPubKeys to 34 bytes, script-argument witness items to 256 bytes, and restricting Tapscript features that can facilitate data embedding, such as OP_IF, OP_NOTIF, and OP_SUCCESS* opcodes, BIP-110 argued that it could prevent many mainstream methods from inserting arbitrary data into Bitcoin. As part of the soft fork, UTXOs created before activation would remain spendable, but outputs created by transactions relying on features prohibited under BIP-110 could become unspendable.

under the temporary rules until the restrictions expired. The soft fork was designed to remain active for approximately one year, an intentional expiration meant to avoid permanently removing Taproot features or permanently stranding funds that conflicted with its restrictions. BIP-110 was not proposed as a permanent redesign of Bitcoin but as a temporary intervention intended to demonstrate whether stronger consensus-level restrictions could meaningfully suppress arbitrary-data use. Despite this, BIP-110 failed to gain significant miner support outside of a small number of committed participants. Its limited adoption ultimately highlighted one of the central difficulties facing any UASF: even if users can independently enforce stricter consensus rules, the fork's practical viability depends on attracting enough economic and mining support to sustain a usable chain. At the very start of the mandatory signaling period, BIP-110 nodes rejected block 961,632 mined by the Antpool mining pool. Shortly afterward, Roughnecks, a mining group operated within the OCEAN mining pool, successfully mined a BIP-110-valid block, permanently splitting the chains, though the BIP-110 branch would only produce a handful of blocks before stalling.

III. The Arbitrary Data Debate

Within just a few years after Bitcoin's genesis block, users were already filtering transactions they considered spam. Starting with SatoshiDice in 2012, a gambling service that flooded the network with small transactions until its creators fixed the issue due to the concerns raised by the network, the Bitcoin community's disputes have always followed the same motions we see today: disagreements on whether filtering counts as censorship, whether it accomplishes anything when other nodes accept it, and how a node operator should treat a transaction they believe harms the network. When OP_RETURN came in 2014, it became a somewhat successful compromise for nearly a decade. Beginning in 2023, though, inscriptions and the Ordinals numbering scheme absolutely took off in popularity, exploiting the cheap witness field to write images and token ledgers onto the chain at a commercial scale. Fees spiked over extended periods, and the UTXO set skyrocketed compared to its original trend. Node operators witnessed firsthand that the relay policy alone had failed as a deterrent for exploitative arbitrary data insertions, and many started to deliberate if something more binding were plausible and justifiable. Others, like Core's development team, instead viewed this time as proof that the limit was doing nothing to deter non-monetary data and was instead pushing data towards the locations that cost the network and node operators the most.

Those conclusions collided in 2025 after Core proposed removing the OP_RETURN relay limit that spring, and critics accused Core of attempting to normalize spam and raised concerns about the legal exposure of node operators that now face the risk of relaying high-fidelity illicit material that the original 83-byte relay limit did not allow for. Despite the controversy, Core released version 30, which implemented this change, in October 2025, and the alternative node implementation, Bitcoin Knots, surged in adoption as a protest from the community. BIP-110 was later introduced as a direct response to Core V30, aiming to push the 83-byte limit back into

existence by forcing it into consensus, all while attempting to disable many of the arbitrary data insertion methods described previously. An OCEAN miner found the first signaling block in March, and despite the passionate surge in Knots' usage, at one point becoming upwards of 25% of node operators, BIP-110 was backed by very little hashrate support, estimated to only be about 2.5% of the total work of the network. Once mandatory signaling occurred, the BIP-110 chain rejected all blocks that failed to signal, leading to a chain split, with the BIP-110 chain crawling to a halt due to low miner support and its supporters planning to relaunch it as a separate network with a different mining algorithm.

IV. The Two Philosophies

Before highlighting the differences, it is important to establish that these two schools of thought in Bitcoin align on most, if not all, of Bitcoin's common ground; both projects value open-source development, long-term security, affordable verification through independent node operators, and Bitcoin's goal to serve as a superior money compared to centralized and inflationary monetary systems. This disagreement instead concerns which of these shared properties should be preserved when they come into question, and which forms of intervention ultimately strengthen or undermine them.

Bitcoin's rules can define what is valid, but they cannot define what Bitcoin is for. Whatever protects Bitcoin's purpose therefore must live outside of the software, and there are currently two competing mindsets of what this protection should consist of. To understand this divide at its source, this research turned to two Bitcoiners who approach the question with entirely different perspectives: Chris Guida, one of BIP-110's most committed defenders, and Shinobi, one of anti-spam policy's strongest critics. Each was asked the same underlying question: if the code cannot encode what Bitcoin is for, what does, and what, if anything, should it protect?

Chris Guida:

"Bitcoin can encode rules for valid blocks and transactions, but it cannot encode the principle that Bitcoin is money. That principle has to live in its culture, because culture is part of Bitcoin's security model. If bitcoiners stop valuing and defending Bitcoin as universal, decentralized money, then the rules themselves can gradually be changed or reinterpreted until inflation, censorship, or other compromises become acceptable. Bitcoin does not protect itself; its users have to continually defend it against the political and economic incentives created by the money printer it was meant to replace." (C. Guida, personal communication, August 26th, 2026)

Shinobi:

"Bitcoin is ultimately a complex system, and systems function how they function in the real world, not how people wish them to function. Any rational approach to Bitcoin must take this

reality into account, or it is not a mode of scientific engagement or thinking; it is one of dogma." (Shinobi, personal communication, August 20th, 2026)

While starting from the same problem, Guida and Shinobi offer far different beliefs on what is needed to protect Bitcoin. Guida believes it is culture, viewing the will of Bitcoiners to defend Bitcoin as money as a critical component of its security model rather than a preference, warning that a community that stops defending that principle will eventually watch these rules be twisted over time. Shinobi believes in Bitcoin's logical accuracy, insisting that any approach not grounded in how the monetary system actually behaves has failed in engineering and instead has become belief. This debate is a disagreement between two philosophies that view Bitcoin fundamentally differently, which explains why a decade of technical debate has never brought the arbitrary data debate to a settlement or conclusion.

The Core Philosophy

Core maintains that Bitcoin's primary goal should be to remain a neutral, censorship-resistant system where all consensus-valid transactions are never judged by their purpose or form. Under this view, the network neutrality that allows for permissionless transactions to be moved efficiently and confirmed independently is Bitcoin's greatest strength, and that property can only be maintained if it's held unconditionally. Neutrality is not indifference to what people do with Bitcoin, but instead a deliberate refusal to support a system that would force anyone to care. In the topic of spam, a similar conclusion is established by Core: because a node can never perfectly know in advance which data is arbitrary or monetary, it can never reliably prevent arbitrary data. Arbitrary data is not a policy failure that better software can fix, but instead an unpreventable consequence of information theory, and Core acted on that reality by raising the OP_RETURN relay limit in Version 30. If data cannot be prevented, the only remaining question is where it will end up and what the best-case scenario would be for it. Core treats node costs as an engineering problem instead of a problem for policy to solve. Their solutions involve improving pruning and increasing node performance through quality open-source development. Under this philosophy, arbitrary data becomes a non-issue when one understands that so long as transactions meet consensus and pay a fee, Bitcoin is working as intended, including the risks associated with illicit material that have been stressed by their opposing side.

Core supporters treat the risk of illegal material on the blockchain as a genuine concern in principle but one that has already been tested in practice. Such material has existed on Bitcoin in various forms for more than a decade without producing the legal catastrophe some anticipate, which Core reads as evidence that the threat has already been measured against the reality by lawmakers, the market, and an informed public. For example, a node operator relays and verifies data regardless of their support for it. While this is a common complaint from node operators regarding arbitrary data, it also frames a legal argument against their liability for that same data. A node operator relaying data acts far more like an infrastructure provider than a publisher, an

analogy supported by the Supreme Court's reasoning in *Twitter, Inc. v. Taamneh*, 598 U.S. 471 (2023), which declined to treat providers of generally available communications infrastructure as culpable merely because bad actors used their services for unlawful purposes. Core-aligned Bitcoiners argue that prosecuting a node operator for material passed through their machine would be unjust and ineffective at addressing the underlying harm, especially when the open blockchain that node operators broadcast preserves a permanent record that may help investigators identify the responsible party through blockchain forensics. The illicit-material segment of the arbitrary data debate presents the hardest test of Core's neutrality values. If censorship resistance is abandoned when the content being resisted becomes sufficiently objectionable, then neutrality is not a property of Bitcoin but a privilege extended only to acceptable uses. Core's philosophy accepts the uncomfortable reality of that conclusion, even for the most objectionable of data. While it should go without saying, Core supporters do not claim such data deserves protection, but that Bitcoin's unwavering censorship resistance does. They maintain that the network cannot weaken one without weakening the other.

The Knots Philosophy

Knots supporters believe Bitcoin's primary goal should be to serve as accessible, sound, peer-to-peer money and that the network should actively defend Bitcoin from threats that put Bitcoin's monetary accessibility and use case at risk. In Knots' view, the software defaults and consensus should actively discourage high-volume non-monetary data with the goal of protecting the network from unnecessary data and potential attack vectors. Neutrality, under this philosophy, is only for genuine monetary transactions on blockchain, not false transactions that embed data and exploit node operators for cheap data storage. According to Knots, Bitcoin was created to be a decentralized, finite, and unconfiscatable monetary system: the perfect money, and to ensure Bitcoin's future as perfect money, it has to be actively defended from misuse. By extension, Knots supporters view arbitrary data as a mispriced cost to the network. When a transaction embeds data on Bitcoin, the miner who got it in a block is paid once. Every node operator, current and future, then carries that data indefinitely in storage and verification cost with zero compensation. The fee market prices in the valuable work of the miner but does not price in at all what the network absorbs when a permanent UTXO of arbitrary data is added to the set. Knots contends that the free market is failing to charge "spammers" for the cost to the network and believes that artificially creating that cost is possible by shifting Bitcoin to an anti-spam culture. By maintaining a unified distaste for non-monetary data and creating soft forks to disable current and future spam methods, the Knots community imagines a world where commercial-level arbitrary data projects in Bitcoin fizzle out due to increased overhead costs in development and fees, increasing risk and therefore discouraging this business in Bitcoin. Knots users point to moments like Vitalik Buterin after his "ultimate scripting" proposal for Mastercoin was not adopted as evidence that communities can push experimental use cases that they believe do not align with Bitcoin toward separate systems (Jacobetty & Orton-Johnson, 2023).

On illicit material, Knots holds the opposite conclusion as Core. They view such content as an unresolved attack vector rather than a known risk, claiming the harm can reach far beyond persecuting node operators. They believe the material can be used as a weapon against Bitcoin in the eyes of policymakers, capital markets, and the general public. An attacker only needs to relay and mine something abhorrent into the chain and ensure it hits headlines, which leads to Bitcoin under the spotlight by an audience with little understanding of relay policy or decentralized infrastructure and the risks associated with it. With every moral reason to react badly to what they hear, no one, not even educated Bitcoiners, could blame such a response. Knots believes the community has a duty to do whatever is possible to prevent such an event, as the political and economic consequences risk shifting Bitcoin toward a dark era. With recent market uncertainty and regulatory uncertainty with the Clarity Act, any further distractions from a disastrous publicized event could throw a wrench in what most describe as the Bitcoin machine working just as intended: the lows of the 4-year cycle, a slow deliberation for legal framework, and mainstream adoption on the rise.

The Philosophies Critiqued

After presenting both positions in their own words, it is worth listing the common rebuttals and criticisms both sides have produced on the other. To start, the most common criticism of Core is that its neutrality leads to apathy to these alleged threats to Bitcoin. For example, Knots argues that Core's harm reduction reasoning for the OP_RETURN change does not account for the newfound ability of network defaults to relay large, open-view non-monetary data that can be illicit and harmful in nature. The primary objection is that Core's supposed trust in lawmakers, markets, and the public not to turn against Bitcoin in such an event, or to accept the consequences of such a scenario where they do, is irresponsible and disastrous to Bitcoin's future as a global monetary system. Furthermore, no court has yet ruled on the liability of a node operator, so the future in such a scenario remains uncertain. According to Knots, a bad-acting nation-state with the power to mine a Bitcoin block, encourage legal decisions, and inform mainstream media of the issue currently has the power to taint Bitcoin forever in node and state, with the price likely following suit.

The criticisms of Knots and BIP-110 are equally direct. The primary point is that BIP-110, or any future fork for that matter, will not prevent arbitrary data and locking down the OP_RETURN relay limit reverses the harm-reduction Core implemented in Version 30. Critics also claim the illicit material argument is the weakest justification for BIP-110 rather than one of the strongest as Knots supporters claim, since such content predates the BIP and Core V30 by over a decade. Furthermore, restrictions on Tapscript go beyond blocking routes for data storage, since some wallets are built on current script behavior that would be disabled for a year under BIP-110 activation, leading to temporary loss of funds. While Knots claims this threat is overblown and the number of wallets affected is far smaller than critics imply, even one instance

of a user temporarily losing funds because of BIP-110 would insult Bitcoin's unconfiscatable ethos.

Core and Knots' positions can be summarized into specific guidelines and compared head to head, highlighting their philosophical gap and conflicting values for Bitcoin in plain view.

Criteria	Bitcoin Core	Bitcoin Knots and BIP-110
Primary purpose and priorities	A neutral, censorship-resistant settlement network. Does this preserve Bitcoin's neutrality?	Accessible, sound money that should discourage arbitrary use cases. Does this preserve Bitcoin as money?
What protects the network	Markets. Incentives, competition, and fee markets deter inefficient uses over time.	Nodes. Operators should discourage non-monetary data, because a free market alone has not priced its full cost.
Node accessibility	An engineering problem. Prune better, verify faster, and use inexpensive refurbished hardware to solve.	A policy problem. Node cost is akin to a user right, and the community should defend it wherever possible.
Illicit content risk	Tested and survivable. Such material has existed on-chain for over a decade, and infrastructure liability generally requires awareness and intent.	An unresolved attack vector. Direct liability may be limited, but reputational, political, and market consequences are real.
Effectiveness of filtering	Futile. Restricting one route pushes data toward worse routes, including permanent UTXO bloat.	Partial effectiveness works. The goal is to raise cost and risk for industrial-scale operations.

V. The Evidence

While philosophies, values, and ideas for Bitcoin and its future differ, the numerical evidence of Bitcoin's state is not in dispute. Both sides acknowledge running a node has become increasingly more demanding, especially since Taproot and inscriptions. Because these costs can be estimated through blockchain data, they can be verified directly with a personal node, and the measurements listed were confirmed directly with one for this research. The blockchain and its data change every 10 minutes on average, so readers are encouraged to verify against a current block explorer for verifiable and contemporary information. The first measurements track what it costs to join the network. Initial block download, the process of downloading and verifying the entire chain from the beginning, is the first and most difficult barrier any node operator faces, and it grew far more demanding since 2023 as the average block size surged along with witness data and transaction counts. The second measurement follows the UTXO set, which matters far more per byte than the blockchain size because a pruned node can discard old blocks after verifying them rather than store them, whereas no node can discard the UTXO set. Together, they describe the rising costs of independent verification and Bitcoin's financial sovereignty.

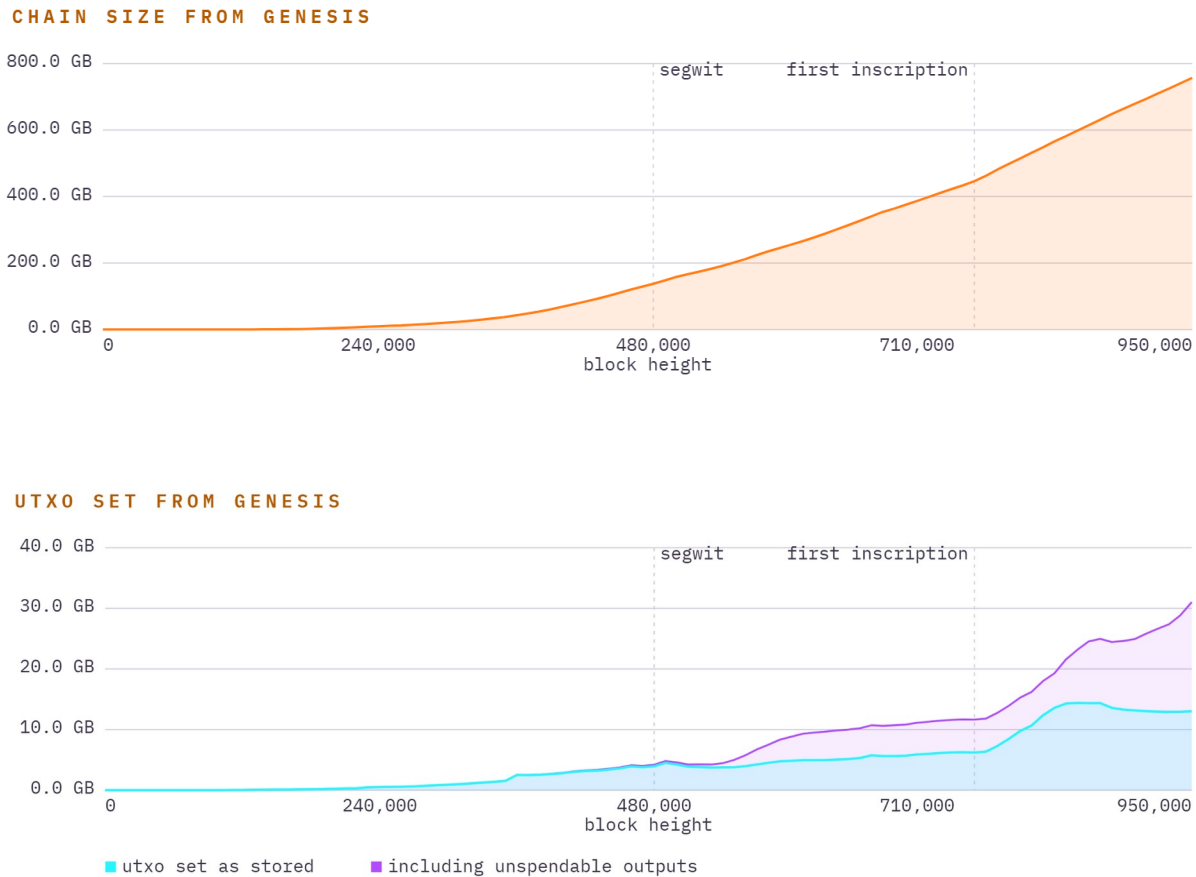


Figure 1. Chain size and UTXO set from genesis to the present, measured from a personal Bitcoin node. SegWit activation and the first inscription are marked for reference. Source: spamwars.connoraherne.com

The stored set triples through the inscriptions era and finally flattens near its peak, while the line including unspendable outputs never flattens at all. This confirms that recent data is largely going to places nodes can discard, which can be presented as proof for Core's harm reduction thesis. Meanwhile, Knots can interpret this data as a scale of the damage, where the flat-lining UTXO set primarily represents the quantity of transaction outputs that will likely sit on every node on the network forever.

While Knots calls arbitrary data destructive to Bitcoin's goals, Core often highlights its benefits to the fee economy. This figure tracks all known methods for arbitrary data to identify its share of blockspace and compares it to the fees attached to the transactions. Both are then weighed against total blockspace and total fees to calculate numerous interesting data points.

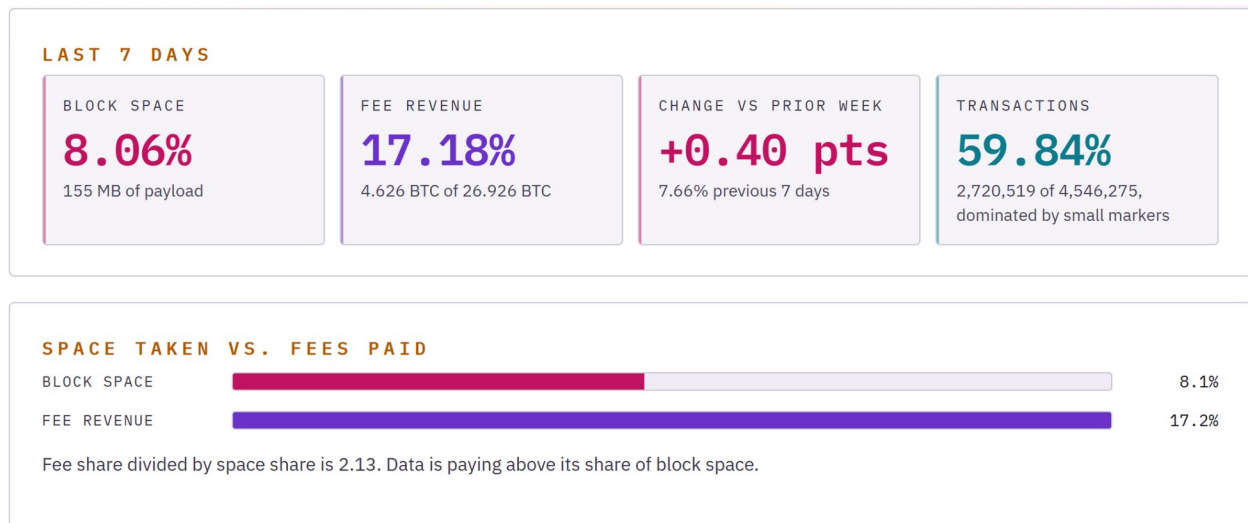


Figure 2. Scale of spam as a proportion of total blockchain data and total fee revenue. Source: spamwars.connoraherne.com

The highlight of Figure 2 is the result affirming that arbitrary data in its current form is paying more for the same blockspace as the average monetary transaction.

VI. The Three Fronts

Bitcoin's network has, essentially, chosen Core, but it's important to be precise about what this means for consensus. Core's position prevailed by default rather than argument due to BIP-110's aggressive activation structure starting with mandatory signaling. Despite this, Core's answer to the non-monetary data concerns is now the only one the dominant chain has.

The Node

With BIP-110 defeated, the individual's cost of verifying the Bitcoin network and address balances is left entirely to the free market, which is exactly what Core argued it should be, allowing for their harm reduction thesis to be freely tested in plain view, verifiable by any node. If the numbers and charts cited continue to climb at an accelerated rate, it will be clear that the concerns raised by Knots and BIP-110 supporters were well founded, and they will likely reappear to form the next wave of the arbitrary data debate. One thing that remains certain is that self-custody and verification will always come at a cost. Nothing proves this more than what occurred a week before BIP-110's mandatory signaling period: the Coldcard hack. Beginning July 30th, 2026, a Coldcard firmware vulnerability implemented and unnoticed since the 2021 release allowed attackers to reliably reconstruct the private keys of a Coldcard without even touching the device, draining over 100 million dollars in Bitcoin from over 5,000 addresses at the time of writing. This flaw was summarized as a failure of verification, complacency, and negligence, with the culture of self-custody suffering for it. While this isn't an inherent flaw in

Bitcoin, it points to the looming threat over financial sovereignty in Bitcoin, which is now under scrutiny and uncertainty on multiple fronts. If the community is to protect the culture of self-verification, it will be crucial to study the coming months of data on the main chain and see how storage and computing costs rise.

The Price

It has been argued on both sides of the arbitrary data debate that the sideways price action that has been witnessed for the three months leading up to the fork could, in part, be from the growing awareness in the broader investing world of the growing conflict within Bitcoin. Just as a CEO and CFO in systemic disagreement would spook investors, a strife between the two largest node implementations of Bitcoin may have played out in capital markets for valuing Bitcoin. With the immediate uncertainty over the soft fork now resolved, what remains is the question of the debate's consequences for Bitcoin. Knots' concerns over node centralization risks and the legal risks of illicit material being embedded in the blockchain remain to be proven as either misguided or correct. On the positive side, the fee economy of Bitcoin continues to benefit from arbitrary data as it pays a premium for blockspace, as shown in figures previously cited. With the status of Bitcoin decided, some participants anticipate a surge in both investor confidence and on-chain transactions. What will occur remains to be seen at the time of writing.

The State

The regulatory front has been critically dissected by both sides of the Core vs Knots debate, sparking discussions on the identity of Bitcoin in the eyes of the state and the legal consequences it could bring. Two critical questions have been formed in this discussion: whether the presence of illegal material on a permanent public ledger creates a genuine legal and political threat to Bitcoin, and what the network would have signaled to the world about itself if BIP-110 had succeeded. The concern of illicit material stressed by Knots deserves attention from policymakers. Imagine the scenario their supporters describe: illegal material placed on the chain, a journalist brings attention to it, and Bitcoin appears in mainstream media headlines beside the worst possible subject matter. The public reaction would be immediate, hostile, and entirely understandable. Legislators would feel pressured to respond, and deliberation over the Clarity Act could slow to a halt. Instead of progress on Clarity, policymakers risk shifting to debating regulations or the legality of distributed blockchain technology after such a disastrous hit to Bitcoin's reputation. It is crucial for policymakers to understand the risks involved and to protect node runners if such an attack were to ever befall the network. On the subject of BIP-110, its activation would have demonstrated something alien to Bitcoin previously: the ability to coordinate the censorship of an entire category of transactions from the open ledger. The previously defensible claims against censoring blacklisted addresses and their transactions, the ability to do so, and the philosophy against it, could both be rendered invalid in the eyes of lawmakers by the activation and success of BIP-110 by proving to authorities that the Bitcoin

network can come together to stop transactions it disagrees with. It has been argued by many that BIP-110 would set a dangerous precedent, and this was likely one of the primary reasons that the network chose differently on August 8th, 2026.

VII. Conclusion and Policy Recommendations

Bitcoin has never succeeded because everyone agreed. Its strength comes from open disagreement, voluntary adoption, and the absence of any authority capable of settling a debate. The arbitrary data debate demonstrated that this property of Bitcoin is still intact, and the resulting disparity and chain split should be seen as the system continuing to function properly. The chain the economy chooses to use will prevail, and the decentralized blockchain's thesis will be strengthened.

This paper set out to explain the divide between Core and Knots and highlight the philosophical wedge in technical priorities. With both sides agreeing on the fundamentals and the data, what remains is the debate of Bitcoin's priorities and the values behind them. As established, the arbitrary data debate is a long-standing dispute in Bitcoin, and it will recur, from SatoshiDice and filtering disagreements of the early 2010s to Core V30 and BIP-110, triggered each time by a new wave of arbitrary data and what it means for the network. Neither implementation is a true victor, as both sides share and prioritize legitimate concerns. Core protects the neutrality that makes Bitcoin worth defending while signaling to policymakers and the public that Bitcoin must not compromise on its neutrality principles no matter what, while Knots identifies a genuine market failure in costs imposed on node operators who never agreed to bear them, a problem that BIP-110's defeat leaves entirely unaddressed.

For policymakers, the following recommendations hold regardless of Bitcoin's future and which side is deemed correct. These can be acted on now rather than waiting for a resolution to arbitrary data that is likely to never arrive.

1. Protect neutral Bitcoin node operators from liability for third-party misuse. A node operator relays and verifies data they do not select, inspect, or curate, which aligns with the experience of an infrastructure provider. Existing legal conclusions in similar cases sided in favor of infrastructure providers, and statutory clarity on node operators specifically would remove the uncertainty currently driving a substantial part of the arbitrary data debate.
2. Target individuals intentionally embedding illicit material, utilizing the open ledger to track and apprehend perpetrators. Do not target the software or the operators that unknowingly relay it. Liability follows awareness and intent, and Bitcoin's design means that operators cannot inspect and remove illicit material from their nodes even if they are to find it and want it gone. This permanent public ledger is an asset to investigators in this scenario, not an obstacle or a threat.

3. Avoid policies that criminalize any decentralized infrastructure. Decentralization does not allow for a primary platform operator, and seeking to find one responsible will either punish no one or the wrong individuals.

Following these recommendations will help preserve Bitcoin's ability to function as open monetary infrastructure. While many early Bitcoin enthusiasts lean towards anti-government philosophies, it is undeniable that the best-case scenario for the world is that the innovation of a decentralized, permissionless, and unstoppable monetary system is supported by all who possess the power to slow it down in its march to financial dominance. No matter the conclusion of short-term debates, a more informed and supportive ecosystem surrounding Bitcoin will further enable its inevitable success across the three defining fronts of node, price, and state.

Acknowledgements

I would like to extend my sincere thanks to the Bitcoin Policy Institute for giving me the credit and support to conduct this research. Specifically, a huge thanks to my BPI mentor, Margot Paez, my fellow research interns, and the BPI leadership for giving me this opportunity. Also, a massive thank-you to the many influential creators and speakers in the Bitcoin community who set aside time and energy from their busy schedules to speak with me about this contentious topic. A specific thank-you to Shinobi, Chris Guida, Matthew Vuk, Pete Rizzo, and Matthew Kratter for their valuable insights, experience, and technical knowledge. Another huge thank you to the attendees of the Bitcoin++ Conference in Toronto from July 22nd-24th that I had the opportunity to connect with for welcoming me into their community and sharing their thoughts on my research. Every experience and connection I have made in the time researching this contentious topic has been memorable and enjoyable.

References

Coin Dance. (2026). *Bitcoin nodes summary*. Retrieved August 26, 2026, from <https://coin.dance/nodes>

Jacobetty, P., & Orton-Johnson, K. (2023). Blockchain imaginaries and their metaphors: Organising principles in decentralised digital technologies. *Social Epistemology*, 37(1), 1–14. <https://doi.org/10.1080/02691728.2022.2086086>