REFLEXIVITY RESEARCH

reflexivityresearch.com

LayerTwo Labs
CUSF V1

LayerTwo Labs

Executive Summary

Bitcoin's protocol upgrade process has slowed sharply since 2017, despite earlier periods of steady improvement through soft forks. Since then, though, only one major upgrade, Taproot in 2021, has been successfully deployed. Bitcoin was founded on principles of stability and security, but the current governance model has introduced a gridlock that makes upgrades increasingly difficult to execute. Informal gatekeeping, high social coordination costs, and reliance on a narrow maintainer pipeline have created a system that struggles to translate technically viable proposals into activated changes. Over time, this dynamic risks leaving Bitcoin less able to respond to technology and the world's ever-changing external pressures.

Core Untouched Soft Forks, or CUSF, propose a structural alternative to the existing upgrade process. Rather than modifying Bitcoin Core, CUSF enables soft forks through external enforcement software that preserves backward compatibility. Participation is voluntary. A soft fork becomes effective only if a majority of miners choose to enforce the new rules, while non-participants remain unaffected. Activation does not require Bitcoin Core maintainer approval or code merges.

By decoupling activation from Bitcoin Core, CUSF seeks to restore permissionless development and reduce governance bottlenecks. Developers can propose and ship upgrades without maintainer approval, miners can coordinate around changes they believe improve network economics, and users retain the choice to participate or abstain. Because enforcement depends on sustained majority support, upgrades can unwind if adoption fades, introducing a degree of reversibility that traditional soft forks lack. This model allows multiple proposals to be tested in parallel while keeping the base client stable.

This governance shift carries tradeoffs. Granting miners a more direct activation role raises concerns about concentration of influence, coordination risk, and social legitimacy. A proliferation of optional upgrades could also increase complexity for users and infrastructure providers. At the same time, the status quo has made certain classes of upgrades, including post-quantum security and expanded scripting capabilities, difficult to advance. This report examines CUSF as a generalized upgrade mechanism, evaluates its benefits and risks, and considers whether it offers a credible path to restoring adaptability within Bitcoin's governance framework.

Bitcoin’s Governance “Problem”

Since its inception in 2008, Bitcoin has been maintained by a globally distributed group of developers contributing to Bitcoin Core and the surrounding node ecosystem. While the project remains open source, a small group of maintainers plays a central role in reviewing, merging, and stewarding changes to the reference client. This structure has helped preserve code quality and security, but it has also concentrated practical influence over protocol evolution.

In the early days of Bitcoin, the protocol was often improved/augmented via technical upgrades. Between 2010 and 2016, the network implemented multiple consensus changes to address concrete issues such as transaction malleability, script limitations, and denial-of-service risks. While these upgrades were cautious, they moved from proposal to activation on a predictable timeline measured in months, not years.

Since 2017, that pattern has broken. Over the past several years, only one broadly scoped soft fork, Taproot, has reached activation. Other proposals with limited scope and clear technical motivation have stalled for extended periods without resolution. This divergence cannot be explained solely by protocol maturity or a lack of ideas. Instead, it reflects a governance environment in which the threshold for change has risen sharply, not only in technical rigor but in social coordination cost and process burden. The contrast between the pre- and post-2016 periods points to a structural change in how upgrades advance.

Protocol Evolution

Source: Paul Sztorc

BITCOIN'S OSSIFICATION

Tracking the declining frequency of consensus changes over Bitcoin's history

Year	2009	2010	2011	2012	2013	2014	2015	2016
#Soft Forks	0*	7	0	2	2	0	2	3

Year	2017	2018	2019	2020	2021	2022	2023	2024
#Soft Forks	1	0	0	0	1	0	0	0 (Presumably)

**Original source code & edit history are mostly lost*

SegWit — 20 Months

- Announced December 2015
- Coded October 2016
- Activated August 2017

Taproot — 46 Months

- Announced January 2018
- Coded October 2020
- Activated November 2021

2.3x Longer

This shift matters because it has normalized inaction/complacency. Bitcoin has adopted a governance structure that makes activation increasingly difficult even when risks are understood, and solutions exist. The result is a system that treats inaction as the default outcome.

No one would argue that stability is not important, but doing nothing for years can also be risky as environments change and technology advances. While the protocol itself aims for long-term stability, the technical and economic conditions around it continue to change. Additionally, while Bitcoin Core maintainers are extremely important for safeguarding the codebase itself, the current governance structure also places significant influence in the hands of a small number of individuals, which can discourage developers from proposing changes that require navigating extended social review and uncertain outcomes.

Some categories of future upgrades underscore this risk. Post-quantum cryptography is frequently cited as a defensive requirement rather than a feature expansion. If advances in quantum computing threaten existing signature schemes, Bitcoin may need to respond within a defined timeframe. Under today's governance process, even widely acknowledged risks can take years to translate into activated changes, widening the gap between threat recognition and mitigation.

Beyond security, limitations in Bitcoin's scripting system also shape what the network can support at the application layer. Modest extensions to expressiveness, such as covenants or improved transaction primitives, have been discussed for years as ways to enable safer vaults, more efficient custody, and better fee management. These proposals often stall not because of unresolved technical flaws, but because the activation path itself is contentious, thanks in part to a growing division in the Bitcoin community as to whether the Bitcoin protocol should do anything beyond moving UXTOs around. When governance friction becomes the primary obstacle, the protocol effectively constrains its own ability to adapt, possibly, one day, to its detriment.

The end outcome is that development slows down. Developers are less likely to suggest changes to protocols because they know that even well-thought-out changes could be stuck forever. This problem is shown by BIP-119 (CheckTemplateVerify, or CTV). The plan was technically sound and received extensive discussion, but it didn't move forward due to issues with the process and cooperation, not because of outstanding technical issues. Unfortunately, the debate ended up focusing on how (and whether) the upgrade should be activated rather than on its actual utility. In many ways, it exposed flaws in Bitcoin's governance framework.

Bitcoin does not require frequent upgrades, but it does require credible mechanisms for acting when circumstances demand it. If meaningful change depends on prolonged coordination within a narrow and high-friction process, the network's capacity to respond becomes uncertain. It is this uncertainty that motivates interest in alternative upgrade mechanisms such as CUSF.

Origin of CUSF

The Core Untouched Soft Fork (CUSF) concept originated from attempts to activate Drivechain (BIPs 300 and 301) under conditions where traditional activation paths proved ineffective. Drivechain proposed a narrowly scoped soft fork designed to enable Bitcoin sidechains while preserving the base layer's security model. The proposal focused on extending Bitcoin's functionality without modifying its core trust assumptions.

Despite extensive technical discussion and refinement, the proposal struggled to progress through the Bitcoin Core process, not because of unresolved consensus flaws, but because of persistent disagreement over the legitimacy of activation and governance precedent.

In response, proponents explored whether a soft fork could be enforced without modifying Bitcoin Core itself. This led to the development of an external enforcement model in which new consensus rules are applied by opt-in software running alongside an unmodified Core node. The central insight was that Bitcoin's consensus model does not require all validation logic to reside within a single client implementation. As long as a majority of miners enforce stricter rules, those rules can become effective at the network level, even if Bitcoin Core remains unaware of them. This pattern became known as a Core Untouched Soft Fork.

What is a Core Untouched Soft Fork (CUSF)?

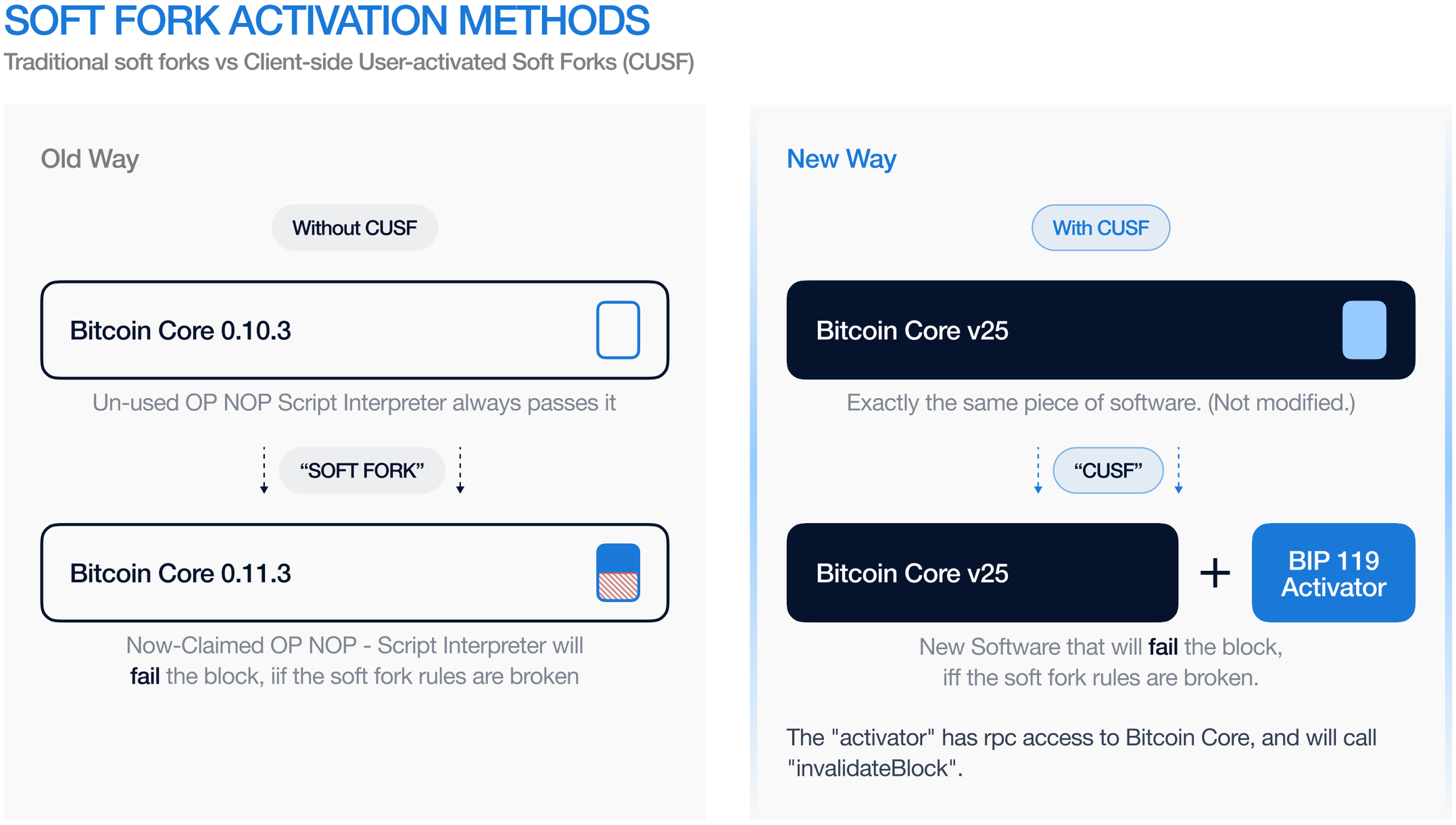
A Core Untouched Soft Fork (CUSF) is a method for activating Bitcoin soft forks without modifying the Bitcoin Core codebase. Instead of merging new consensus logic into Core, CUSF separates rule enforcement into external software, commonly referred to as an activator, that runs alongside a standard Core node. This approach preserves backward compatibility while shifting activation from repository inclusion to voluntary adoption.

In practice, the activator functions as an external validator. It observes blocks produced by the network, evaluates them against the stricter rule set, and instructs the connected Core node to reject blocks that violate those rules. It communicates with Core through standard RPC calls by pulling block data for inspection and (when necessary) instructing the node to reject blocks that violate the new rules.

The key point is that Bitcoin Core does not need to “understand” the new soft fork at all. It remains unchanged and continues operating as it always has. Enforcement happens because the activator tells the node what to consider invalid under the stricter rule set, commonly using workflows built around RPC capabilities such as inspecting blocks and invalidating those that fail the new constraints.

Mechanism Comparison

Source: https://drivechain.info/media/slides/op-next-2024.pdf



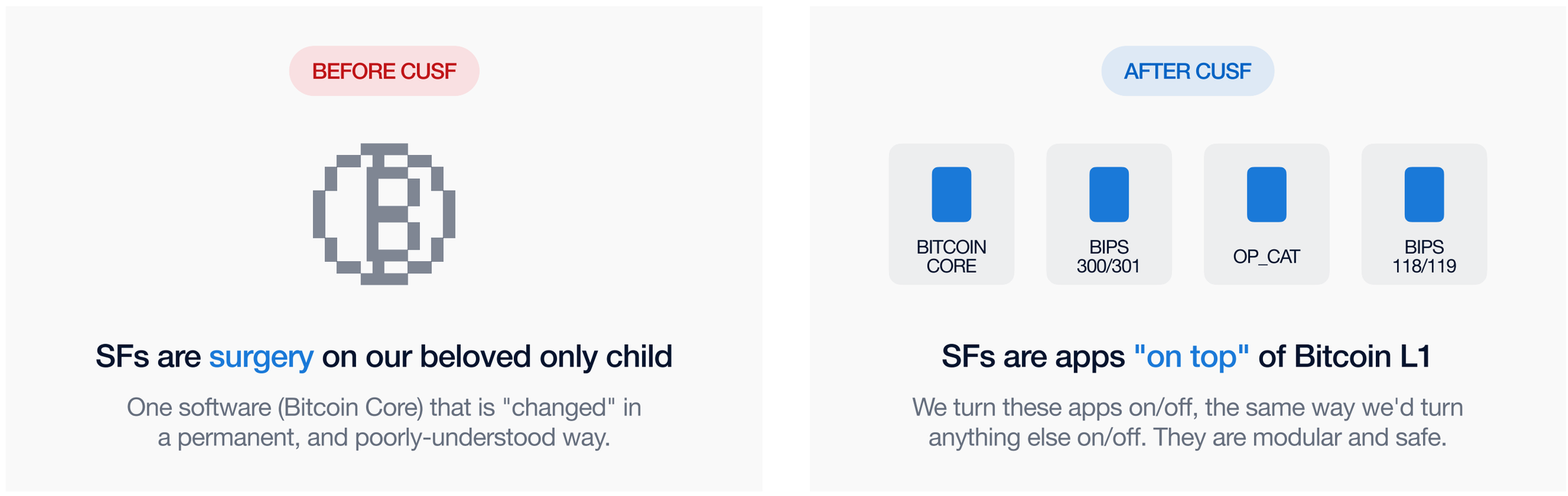
CUSF retains the defining property of a soft fork: participation is voluntary. Miners and nodes that do not run the activator continue validating blocks under the legacy rule set. A soft fork becomes effective only if a majority of miners enforce the stricter rules, at which point blocks that violate them become economically nonviable. At that point, the stricter rule set becomes the de facto standard because the majority chain enforces it, and the network naturally converges on that chain.

Mental Model Shift

Source: https://drivechain.info/media/slides/op-next-2024.pdf

SOFT FORK PERCEPTION

How are soft forks perceived by the layperson?



A Practical CUSF Activation and Deactivation Lifecycle

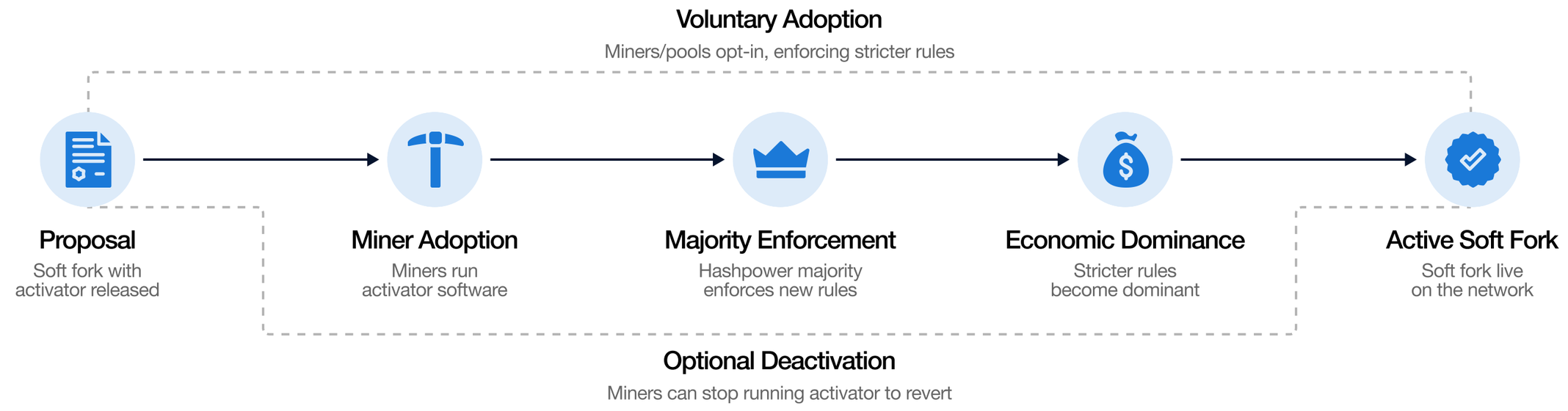
A CUSF follows a different lifecycle from traditional Bitcoin upgrades. Consider a hypothetical soft fork that introduces a narrowly scoped rule designed to improve transaction safety or fee efficiency. Under the CUSF model, a development team publishes external software that enforces the new rules while running alongside an unmodified Bitcoin Core node. No pull request, maintainer approval, or Core release is required.

Activation is driven by miner choice rather than a formal process. Miners or mining pools that believe the proposed rules improve economics begin running the activator software alongside their existing stack. There is no fixed activation date or signaling window. The software can be started or stopped at any time.

Once a majority of hashpower enforces the stricter rules, blocks that violate them become economically nonviable. Miners who do not enforce the soft fork risk producing blocks that the majority chain rejects. At that point, the new rules take effect in practice, even though Bitcoin Core itself remains unaware of them. Users who rely on the new behavior gain stronger guarantees, while non-participants continue operating under legacy assumptions so long as they follow the majority chain.

Activation Process

CUSF ACTIVATION LIFECYCLE



Deactivation is intentionally simple. If miners stop running the activator and enforcement falls below a majority, the stricter rules cease to apply. The network naturally reverts to the prior rule set without requiring a hard fork or emergency intervention. This reversibility distinguishes CUSF from traditional soft forks, which are effectively permanent once activated.

What “Problem” CUSF Solves

CUSF is fundamentally a response to persistent governance inaction. Under the current upgrade process, translating technically viable proposals into activated changes often requires navigating prolonged social coordination, developer bottlenecks, and an increasingly cautious culture around change. Even when proposals address well-understood risks, activation can stall indefinitely. By shifting enforcement outside of Bitcoin Core, CUSF seeks to restore a practical path for experimentation without requiring permission from a small set of maintainers.

The central change is structural. If developers can build an upgrade and persuade miners and users that it delivers value, the upgrade can be attempted without a multi-year effort to secure inclusion in the reference client. Adoption, rather than repository access, becomes the deciding mechanism. This reframes protocol development as opt-in and competitive. Multiple teams can propose alternative solutions in parallel, and market coordination determines which persist.

CUSF also bypasses centralized review as a chokepoint. In the status quo, the practical reality is that if an upgrade is not merged into Bitcoin Core, it is exceptionally difficult to deploy. CUSF removes that dependency. Core maintainers are no longer the bottleneck for activation, because the enforcement software is not asking to be merged into Core in the first place. Instead, responsibility shifts outward and, ultimately, back toward the developers shipping the activator and the miners/users deciding whether to run it.

Opt-in participation further reduces the perceived stakes of upgrades. Because non-participants remain unaffected at the software level, CUSF lowers the risk of coercive or irreversible change. Participants who see value can adopt new rules, while others can continue operating under the legacy model. This flexibility is intended to make experimentation more acceptable without demanding universal agreement up front.

Finally, CUSF introduces reversibility as a governance feature. Traditional soft forks, once activated, are difficult to unwind. Under CUSF, enforcement persists only while the majority support remains. If adoption fades, the network can revert to prior rules without a hard fork or emergency rollback. This creates a softer failure mode that reduces the systemic cost of unsuccessful upgrades.

Advantages of CUSF

The most immediate advantage of CUSF is speed. By removing the need for Core coordination, CUSF compresses the deployment timeline to the time it takes to build credible software and persuade participants to adopt it. Now, this does not eliminate debate, but it removes a structural delay mechanism: the need to secure maintainer buy-in and synchronize around formal release cycles. In a world where Bitcoin may face time-sensitive needs (whether defensive or strategic), CUSF offers a way to reduce upgrade latency.

CUSF also preserves stability at the base layer. Because Bitcoin Core remains untouched, its codebase does not accumulate experimental or proposal-specific logic. Core maintainers are not required to support, patch, or assume responsibility for upgrades they may not endorse. This separation localizes risk to those who opt in and allows the reference client to remain conservative by design.

From a governance perspective, CUSF redistributes activation power. Rather than concentrating influence within a small maintainer group, the model shifts decision-making toward developers who ship usable software and miners and users who choose whether to adopt it. Developers can ship upgrades without permission, miners can enforce them by adopting the activator, and users can choose whether to participate. Nothing is forced, but nothing is gatekept either. The governance center of gravity moves from repository control to adoption dynamics.

Modularity is a core design feature. CUSF treats upgrades as external rule sets layered on top of Bitcoin's base protocol rather than permanent modifications to the client. This modularity improves maintainability and allows multiple proposals to be developed and evaluated in parallel. Competing approaches can coexist, and adoption determines which persist, reducing the need for binary governance outcomes.

Economic alignment is the intended filter. Because activation depends on miner enforcement, proposals must justify themselves in economic terms, including fee revenue, transaction demand, or long-term network value. As block subsidies decline and fee markets become more central to security, this alignment may become increasingly relevant. Upgrades that fail to improve the economic reality of securing Bitcoin are less likely to sustain adoption.

Finally, CUSF emphasizes experimental safety. Enforcement can be discontinued if support fades, allowing unsuccessful upgrades to unwind without hard forks or emergency interventions. This reversibility lowers the cost of failure and reduces the risk of irreversible mistakes, making it easier to test real-world adoption without committing the entire network to a single outcome.

Risk and Counterarguments

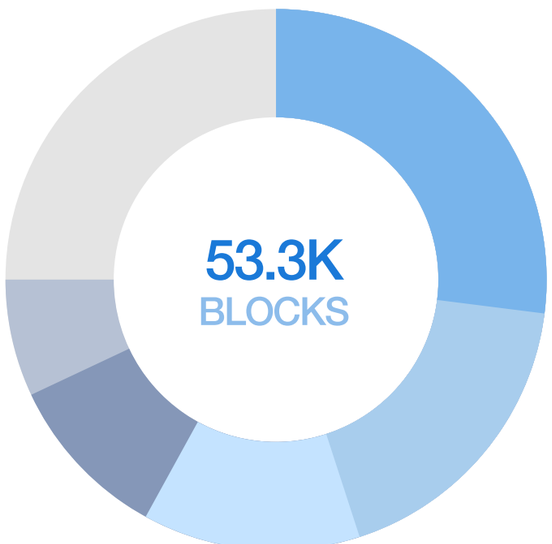
The most direct objection is miner overreach. CUSF effectively makes the majority of the hashpower the activation threshold, raising the fear that miners could push through changes that users do not support. Even if economic incentives discourage reckless behavior, critics argue that granting miners a cleaner activation pathway could upset Bitcoin's perceived power balance, especially for participants who emphasize user sovereignty over miner coordination. That is a real concern.

Bitcoin Mining Pool Distribution, 1-year period

Source: https://www.blockchain.com/explorer/charts/pools

HASHRATE DISTRIBUTION

Estimation of hashrate distribution amongst mining pools (1Y)



Unknown	Antpool	ViaBTC	F2Pool	Others
27,716 (52.0%)	9,714 (18.2%)	6,765 (12.7%)	5,728 (10.7%)	3,397 (6.4%)

The chart shows market share of bitcoin mining pools. It should only be used as a rough estimate. "Unknown' blocks do not indicate an attack-it means the origin could not be determined.

Coordination complexity is a second constraint. CUSF relies on sustained majority enforcement to remain effective. If support hovers near the activation threshold, the network may face ambiguity over whether stricter rules are reliably enforced. For applications or users that depend on those rules, such instability could introduce unacceptable risk unless accompanied by strong monitoring, signaling, and coordination norms.

A third concern is the reduced review surface. Bitcoin Core's caution is often defended as a security feature. Slow review is part of the strategy for avoiding catastrophic consensus failures. By moving enforcement outside Core, CUSF removes one of the highest-trust review pipelines in the ecosystem. That does not mean CUSF cannot be safe, but it does mean safety must be recreated through other means, including audits, open review norms, testing environments, and clear standards around client correctness.

Beyond these stated concerns, another central risk of the CUSF model is fragmentation at the rule level, even if the blockchain itself remains singular. Because upgrades can be enforced externally and adopted on an opt-in basis, different miners may enforce different rule combinations at different times. The question "what rules are active" becomes more dynamic, and the collective mental model of "Bitcoin consensus" becomes less precise. Even if the chain remains one, a proliferation of optional modules could create confusion for users, businesses, and infrastructure providers who prefer a single, stable upgrade narrative. Monitoring which CUSF modules are active, assessing their stability, and communicating that information to users adds operational complexity.

Finally, social legitimacy may be the decisive factor. Even if CUSF works technically and miners coordinate successfully, a contentious activation could provoke backlash from community members who see it as a violation of Bitcoin's social contract. Bitcoin governance is not purely code. It is also about shared norms. If CUSF is perceived as a shortcut around legitimacy, it could create a political fracture.

Outlook & Strategic Implications

CUSF reframes Bitcoin governance as a bottom-up, market-driven process rather than a centralized approval pipeline. In the optimistic case, it restores a credible path for incremental evolution by ensuring that Bitcoin can remain conservative at its base layer while allowing opt-in upgrades to persist openly.

If adopted, this approach could diversify the Bitcoin protocol's development by reducing the reliance on a single repository and single maintainer pipeline. That diversification may improve resilience overall. The idea is simple: letting more teams actually build leads to more ideas being tested. More ideas being tested can lead to new innovations, greater governance scalability, and ultimately a healthier, more decentralized system overall.
At the same time, CUSF does not resolve Bitcoin's governance tradeoffs. It replaces formal process with economic coordination and social legitimacy. Whether this shift improves outcomes depends on how miners, developers, and users respond in practice. Sustained adoption, clear signaling, and shared norms would be required to prevent instability or fragmentation.

The significance of CUSF lies less in any single proposal than in the optionality it introduces. Bitcoin does not need frequent upgrades, but it does need credible mechanisms for acting when circumstances demand it. CUSF offers one possible path for restoring that capability without compromising backward compatibility or forcing universal agreement. Whether it succeeds will ultimately be determined by ecosystem acceptance rather than design alone.

Disclaimer

This report was commissioned by LayerTwo Labs. This research report is exactly that — a research report. It is not intended to serve as financial advice, nor should you blindly assume that any of the information is accurate without confirming through your own research. Bitcoin, cryptocurrencies, and other digital assets are incredibly risky and nothing in this report should be considered an endorsement to buy or sell any asset. Never invest more than you are willing to lose and understand the risk that you are taking. Do your own research. All information in this report is for educational purposes only and should not be the basis for any investment decisions that you make.

REFLEXIVITY RESEARCH

“

Our mission is to bridge traditional finance into digital assets through our crypto native research.