

Analyzing Bitcoin Consensus: Risks in Protocol Upgrades

RenCryptoFish

November 6, 2024

Read the full paper →

This paper provides an analysis of bitcoin's consensus mechanism, focusing on the roles of various stakeholders, their powers, and the incentives that guide their actions. Bitcoin is incredibly difficult to change by design. The default is no change. Any significant change needs to pass that hurdle.

1 The Nature of Bitcoin Consensus

Bitcoin's consensus mechanism extends far beyond the technical protocol. It encompasses a social and economic process where multiple stakeholder groups must align before any change can be implemented. The system is deliberately conservative — the status quo has a built-in advantage, and any proposed modification faces significant resistance by default.

This conservatism is a feature, not a bug. It protects the network's core properties: fixed supply, censorship resistance, and permissionless access. The difficulty of changing Bitcoin is what makes these guarantees credible.

2 Six Stakeholder Groups

We categorize the roles people play in bitcoin's consensus into six distinct stakeholder groups, each with their own motivations and influence:

1. **Users** — Individuals and entities who hold and transact in bitcoin. They ultimately determine which version of the software (and thus which rules) they accept. Users express preferences through the software they run and the chain they recognize as valid.
2. **Miners** — Entities that expend computational resources to produce blocks. Miners have direct influence over which transactions are included in blocks and can signal support for or against proposed changes. Their economic incentives are tied to the value of block rewards and transaction fees.
3. **Bitcoin Core Developers** — Contributors who write, review, and maintain the reference implementation. They propose and implement technical changes but cannot force adoption. Their influence comes from expertise and trust rather than formal authority.
4. **Bitcoin Core Maintainers** — A smaller subset of developers with merge access to the repository. They serve as gatekeepers for the reference implementation. Notably, while Bitcoin Core maintainers do not have excessive power to change Bitcoin, they possess significant power to veto changes.

5. **Economic Nodes** — Exchanges, payment processors, and other businesses that validate transactions and enforce consensus rules. These entities have outsized influence because they determine which chain has economic activity and liquidity.
6. **Investors and Speculators** — Market participants whose capital allocation decisions signal confidence in (or concern about) proposed changes. Market reactions can accelerate or derail consensus processes.

3 Shifting Power Dynamics

The relative powers of the stakeholders shift depending on their role in the network's operation and the stage of the consensus change process. During normal operation, miners and economic nodes have the most direct influence on the network. During a proposed consensus change, the dynamic shifts:

- **Proposal stage:** Developers and technical contributors dominate the conversation, as changes must first be coherent at a technical level.
- **Debate stage:** Users, businesses, and investors become more influential as the discussion moves from technical feasibility to economic and philosophical desirability.
- **Activation stage:** Miners and node operators become critical, as they must actually run the new software for a change to take effect.
- **Post-activation:** Users and economic nodes ultimately decide whether the change "sticks" by choosing which chain to recognize and transact on.

4 The Veto Power Asymmetry

One of the key findings is the asymmetry between the power to propose changes and the power to block them. Bitcoin Core maintainers illustrate this clearly: while they cannot unilaterally push changes onto the network, their gatekeeping role over the reference implementation gives them substantial veto power. A change that is not merged into Bitcoin Core faces a much higher barrier to adoption, even if it has broad community support.

This asymmetry exists at every level. Any stakeholder group can effectively veto a change by refusing to adopt it:

- Miners can refuse to signal for activation
- Economic nodes can refuse to upgrade their software
- Users can continue running old versions
- Developers can refuse to implement or review proposals

The result is that consensus changes require broad, multi-stakeholder agreement — a high bar that protects the network but also makes beneficial upgrades slow and contentious.

5 State of Mind

We also introduce the concept of **State of Mind**, which affects the degree that stakeholders engage in the process of finding consensus. Stakeholders exist on a spectrum from fully engaged to completely passive:

- **Active participants** closely follow technical discussions, run test software, and provide feedback on proposals. Their engagement directly shapes outcomes.
- **Passive participants** may hold strong opinions but do not actively contribute to the consensus process. They express preferences primarily through market behavior and software choices.
- **Unaware stakeholders** may not even know a consensus change is being proposed. Their inaction defaults to supporting the status quo.

The State of Mind concept is important because it highlights that consensus is not a simple vote. The intensity of preference matters as much as the direction. A small group of deeply engaged stakeholders can have more influence than a large group of passive ones, for better or worse.

6 Implications for Protocol Upgrades

Understanding these dynamics has practical implications for anyone proposing or evaluating Bitcoin protocol changes:

- **The burden of proof is on the proposer.** The default state of "no change" means that any proposal must demonstrate clear, compelling benefits that outweigh the risks of modification.
- **Technical merit is necessary but not sufficient.** A change must also navigate the social and economic consensus process, which requires buy-in from multiple stakeholder groups with different incentives.
- **Activation mechanisms matter.** The choice of how a change is activated (flag day, miner signaling, user-activated soft fork) affects which stakeholders have the most influence and can change the outcome.
- **Patience is required.** Bitcoin's consensus process is deliberately slow. Attempts to rush changes face resistance from the system's conservative design.

The difficulty of changing Bitcoin is its greatest strength and its greatest challenge. It ensures that the network's fundamental properties remain stable, but it also means that even widely desired improvements can take years to implement. Understanding the roles, powers, and incentives of each stakeholder group is essential for navigating this process effectively.