Analyzing Bitcoin Consensus: Risks in Protocol Upgrades

Ren Crypto Fish, Steve Lee, Lyn Alden

Motivation

- Bitcoin is hard to change, a property that is critical to it having any value at all

- But what keeps it from changing?

- If we want to improve bitcoin, how can that be done and what risks might it present?

BCAP non-goals

1. To take a perspective on whether bitcoin should change or how fast it should change

2. To advocate for any particular change

3. To be become a blueprint for how to change consensus

Contributions from the paper

1. We identify six distinct stakeholder groups with their own powers and incentives to maintain and influence bitcoin consensus
2. State of Mind of stakeholders and its impact on the consensus change process
3. The relative powers of the stakeholders shift through the consensus change process
4. Bitcoin Core developers have veto(ish) power on consensus changes
5. Adopting Alternative Consensus Clients can lead to a fragile network and risks chain splits and bounty claims
6. Not all Investors are equal during price discovery of a contentious consensus change

Who are the stakeholders?

Investors

They include:
- Large individual holders of bitcoin
- Active and passive institutional fund holders of bitcoin
- Sovereign wealth funds, central banks, and governments

Powers:
- Influence market prices through buying and selling activity
- Signal preferences for different proposals through futures markets
- Fund development efforts or advocacy for specific changes

Incentives:
- Maximize the value of their bitcoin holdings
- Maintain or improve bitcoin's properties as a store of value
- Minimize risks of network instability or contentious changes
- Comply with regulatory requirements in their jurisdictions
- May have equity investments in bitcoin businesses

Segments of Investors

Type	Self Custody	Institutional	Corporation	ETF
Custody	Self	QC	QC	QC
Ownership	Self Owned	LPs GPs	Board of Directors, Shareholders	ETF Sponsor Executives of Issuer
Ability to Act Quickly	High	Medium	Low - Medium	Low - Medium

Economic Nodes

They include:
- Cryptocurrency exchanges
- Payment processors
- Custody providers
- Large merchants and service providers who accept Bitcoin as payment
- RPC providers (manage and host nodes for application developers)

Powers:
- Ability to define which fork is bitcoin by choosing which version of the software to run and set ticker symbols
- Reject blocks they consider invalid, potentially causing chain splits
- Ability to list or not list markets for spot and derivative markets for forks
- Ability to sell fork coins on behalf of users without their permission

Incentives:
- Maximize transaction volume and trading activity
- Maintain the security and stability of the network
- Comply with regulatory requirements in their jurisdictions

Media Influencers

They include:
- Media and press organizations
- Thought leaders with large followings on social media platforms
- Organizers of conferences related to bitcoin

Powers:
- Shape narratives around bitcoin and proposed changes.
- Distort the perceived support level of a consensus change (either aggrandizing or minimizing) relative to reality.
- Amplify or critique various stakeholder positions.
- Educate the broader public about bitcoin developments.

Incentives:
- Generate engagement and grow their audience.
- Maintain credibility within the bitcoin community.
- Act in their sponsors best interest.
- Often have their own ideological or economic stakes in bitcoin's direction; may fall into one of the other Stakeholder categories.

Miners

They include:

- Individual Miners
- Large scale mining operations
- Mining pools
- Chip manufacturers

Powers:

- Create new blocks, determining which transactions are included
- Signal readiness for protocol changes through version bits
- Potentially censor transactions by not including them in blocks
- Direct hash power to compete for chains in the event of a fork. Each ASIC mining chip can only mine for one side of a fork

Incentives:

- Maximize revenue from block rewards and transaction fees
- Maintain the value of their specialized hardware investments
- Avoid network instability that could threaten the value of bitcoin

Protocol Developers

They include:

- Developers proposing and implementing consensus changes in addition to maintaining the bitcoin protocol and client(s)

Powers:

- Propose and implement code changes
- Maintain the reference client (Bitcoin Core)
- Provide technical expertise to inform decision-making
- Have veto(ish) power because of how hard it is to grow adoption of an alternative client

Incentives:

- Improve bitcoin's technical capabilities and security
- Maintain their reputation within the developer community
- Often motivated by ideological commitment to bitcoin's principles
- May be incentivized by developer sponsorships

Users and Application Developers

They include:

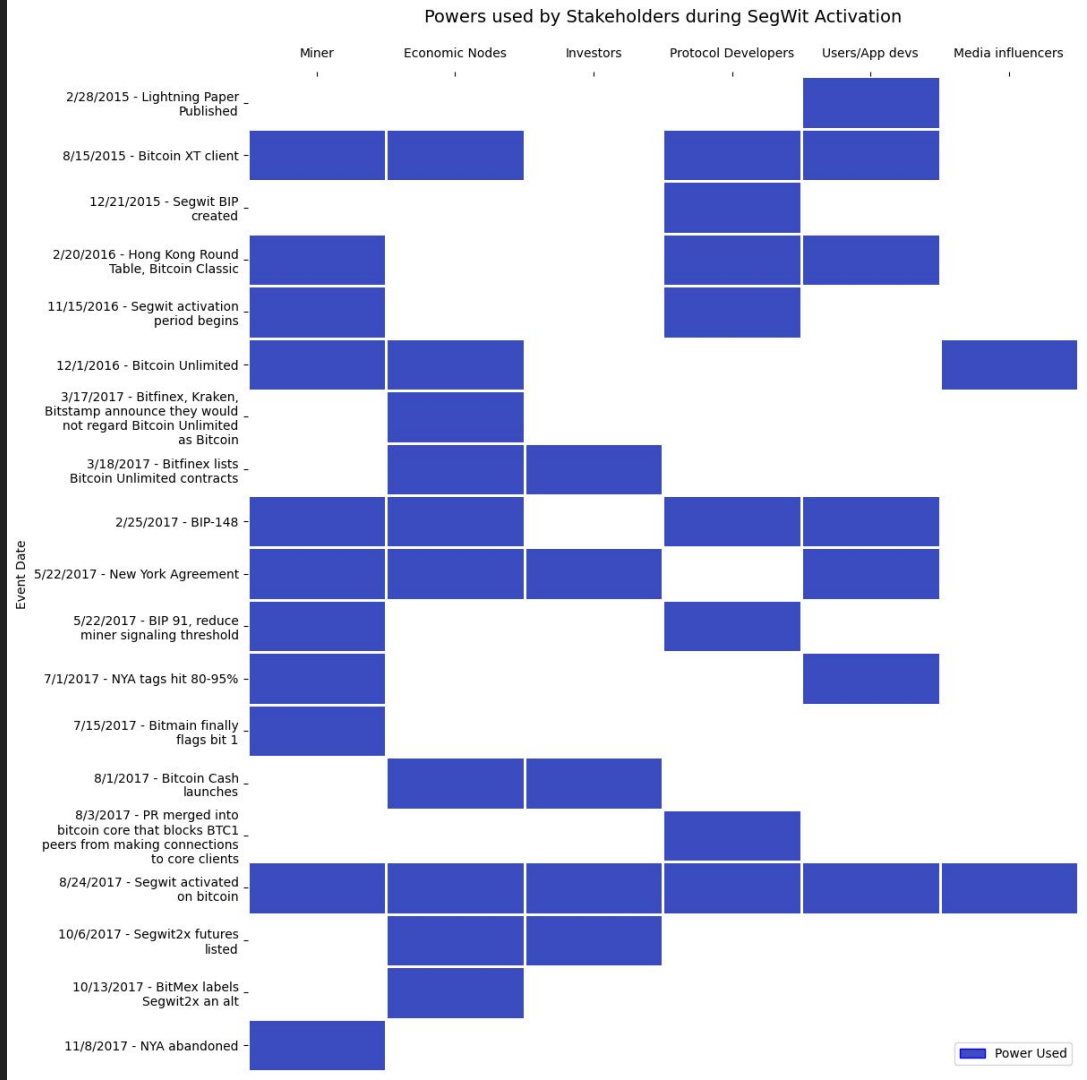
- Users who use bitcoin as a store of value
- Developers and users of payment solutions like Lightning
- Teams working on sidechains or Layer 2 solutions for advanced functionality
- Users and developers of Bitcoin-based DeFi, NFTs or Fungible Tokens applications (e.g., Ordinals, BRC-20, Runes)
- On chain wallet providers
- Equity investors in bitcoin businesses

Powers:

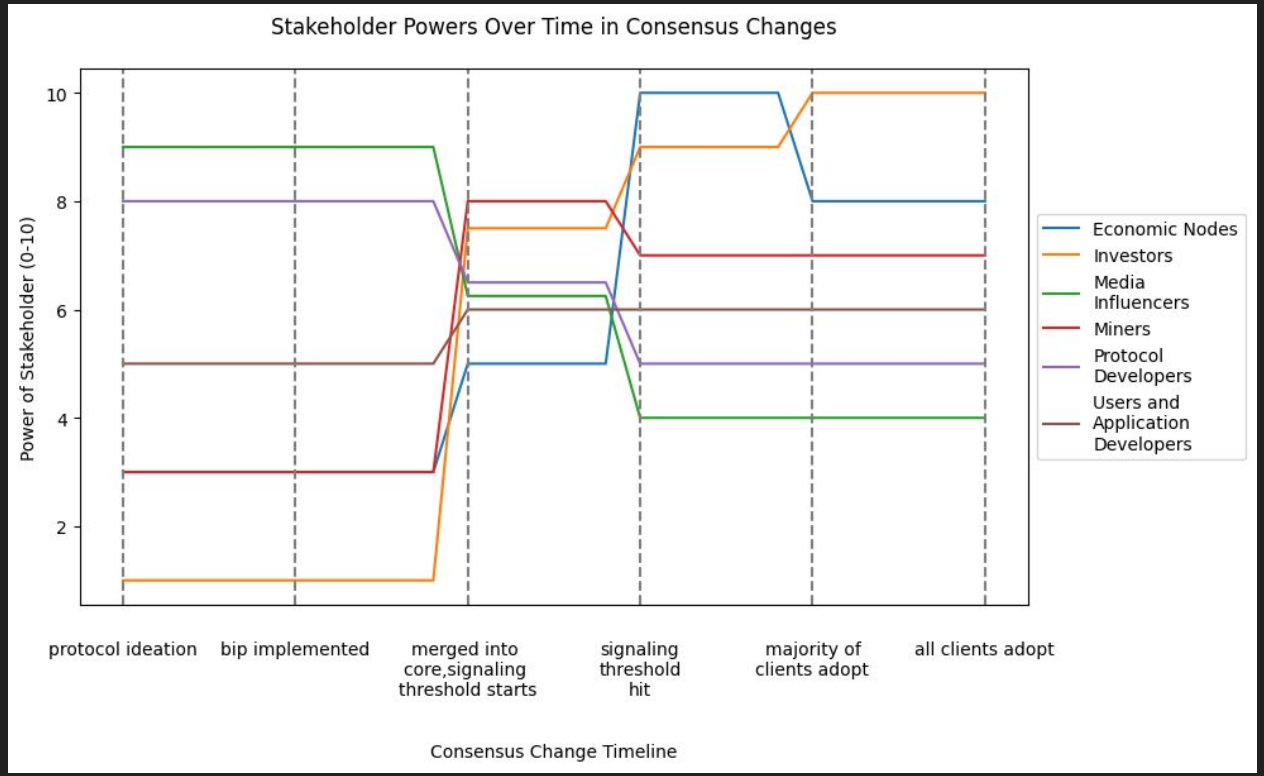
- Often provide the default node connection for users sending and receiving bitcoin transactions
- Sell or threaten to sell one side of a hard fork dispute, but with less scale and impact than Investors.
- Sell or threaten to sell bitcoin and use other cryptocurrencies that meet their needs.

Stakeholders are in a “State of Mind” (SOM)

Segwit showed the complex interplay of powers between stakeholders

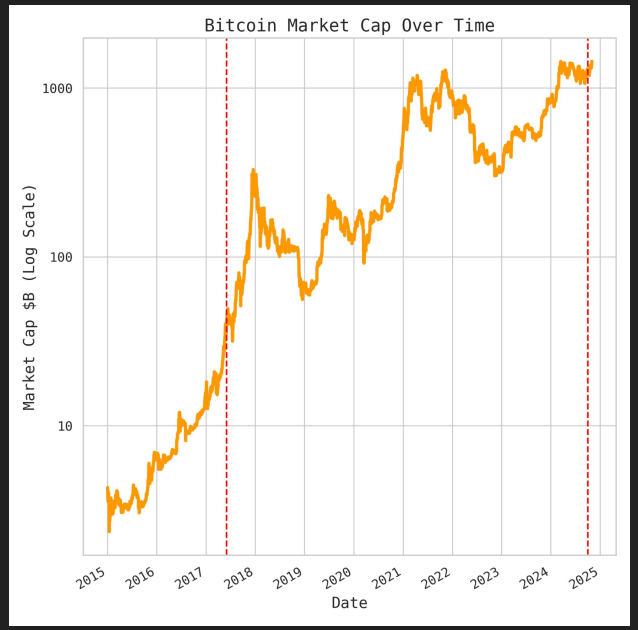


Stakeholders relative powers shift throughout consensus change process

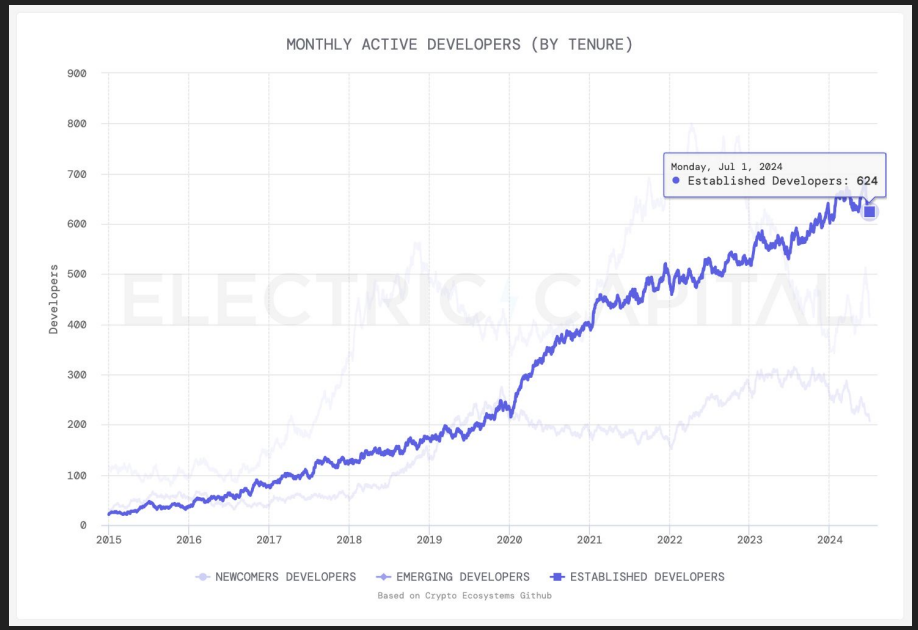


Changing Consensus

Bitcoin is bigger than ever, harder to change than ever, harder to determine when there is consensus



Source: [CoinMarketCap]



Source: [Electric Capital Developer Report]

Historically, all consensus changes have been merged into Bitcoin Core

- Taproot
- Segwit
- CheckSequenceVerify
- CheckLockTimeVerify
- Strict DER signature
- etc…

More consensus change proposals coming from outside of Bitcoin Core maintainers

- Drive Chains
- ANYPREVOUT
- CTV
- TLUV
- Vault
- OP_CAT
- Template Key
- TXHASH
- OP_TX
- CATT
- MATT

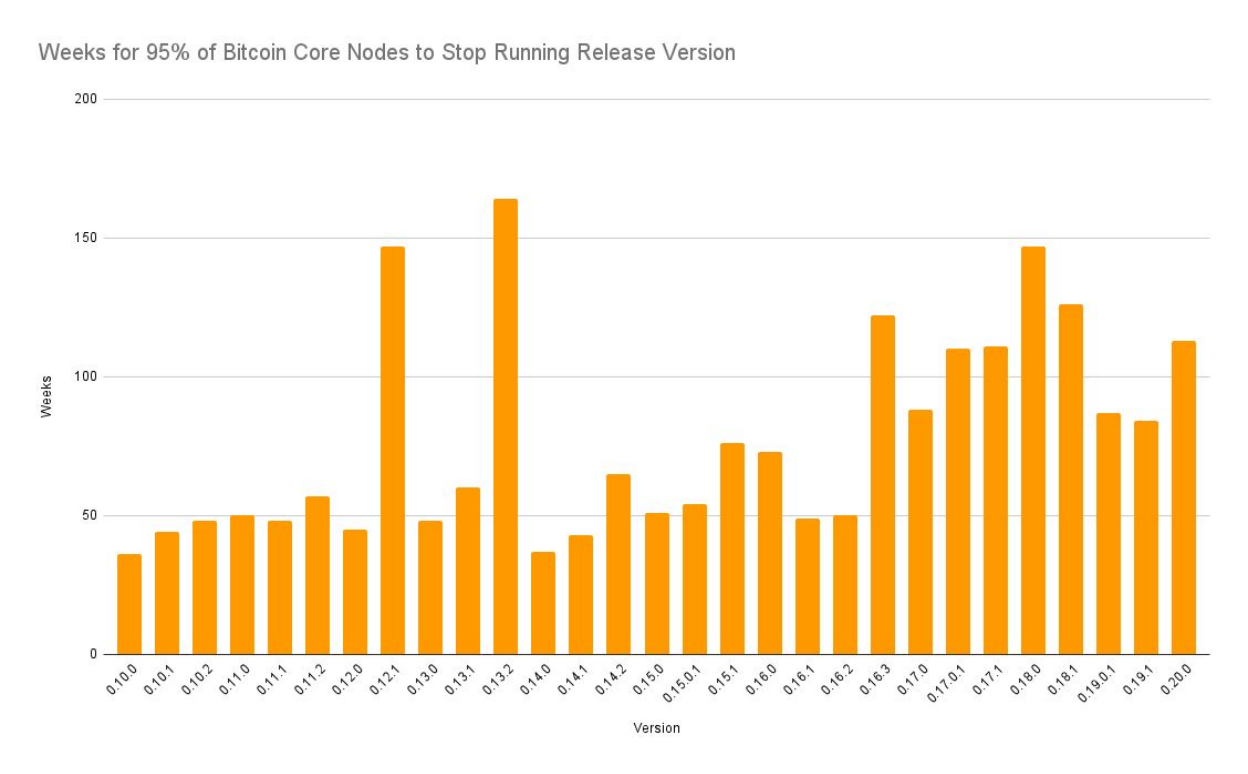
Source: https://github.com/bitcoin/bips, https://covenants.info/

Alternative client adoption is an important option for bitcoin but very difficult to achieve

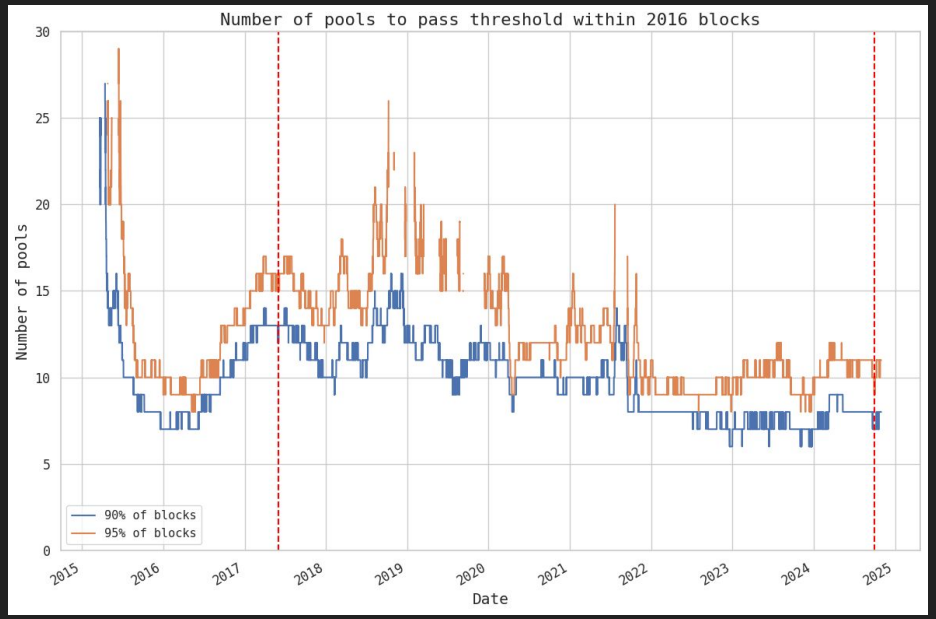
Motivations against adopting Alternative Consensus Client

- **All**: Uncertainty over stability, maintenance, and security of alternative client
- **All**: Why was the change not merged into Bitcoin Core?
- **Economic Nodes**: Risk of fragile network prone to forking
- **Miners**: Performance issues related to peering risk
- **App Devs**: Risk of incompatibility or forks leading to potentially loss of user funds

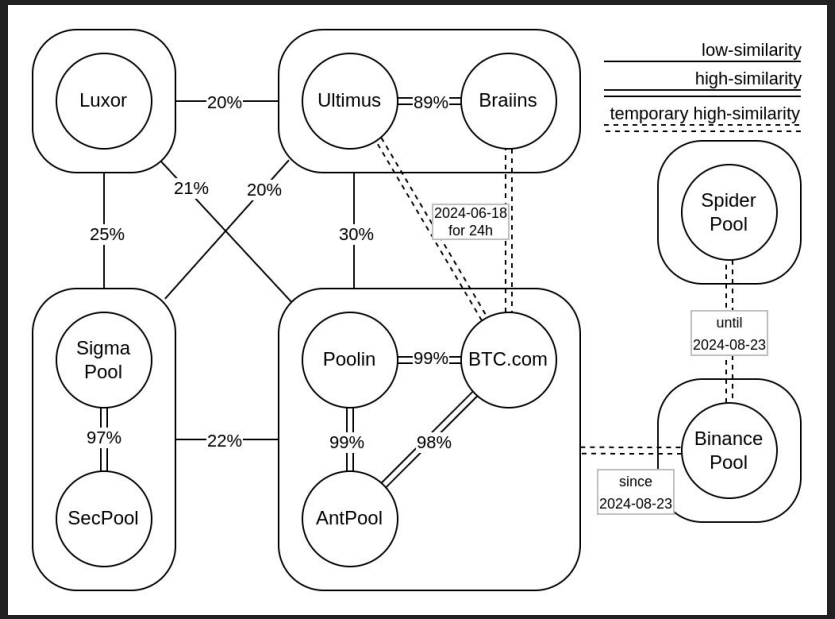
Coordination is hard! It takes ~40 weeks for nodes to upgrade with Bitcoin Core



Mining pools are more centralized than ever



Source: mempool.space



Source: https://b10c.me/observations/12-template-similarity/

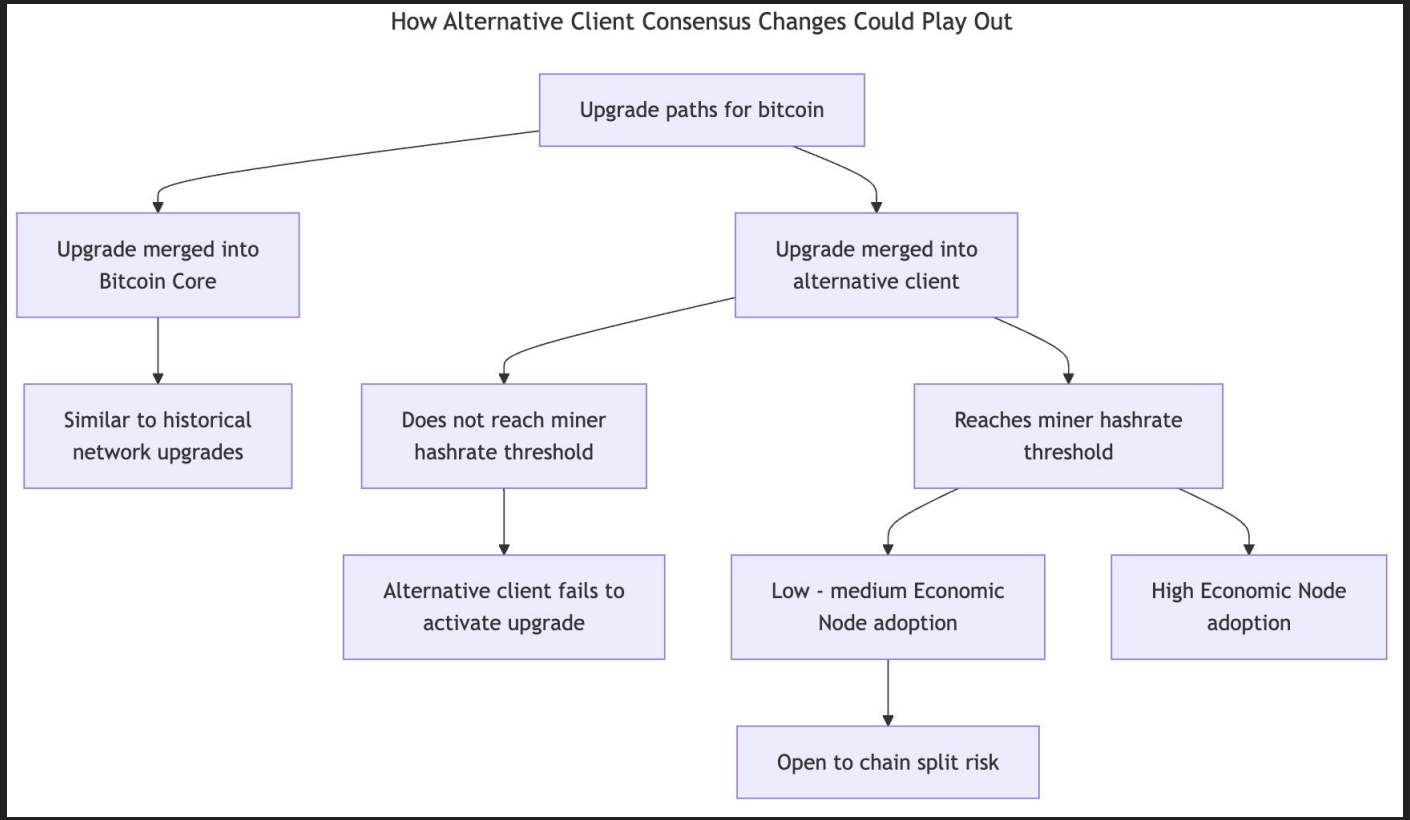
Hash price is at all time lows, miners demanding more fees

Source: Hashrate Index

All this can lead to

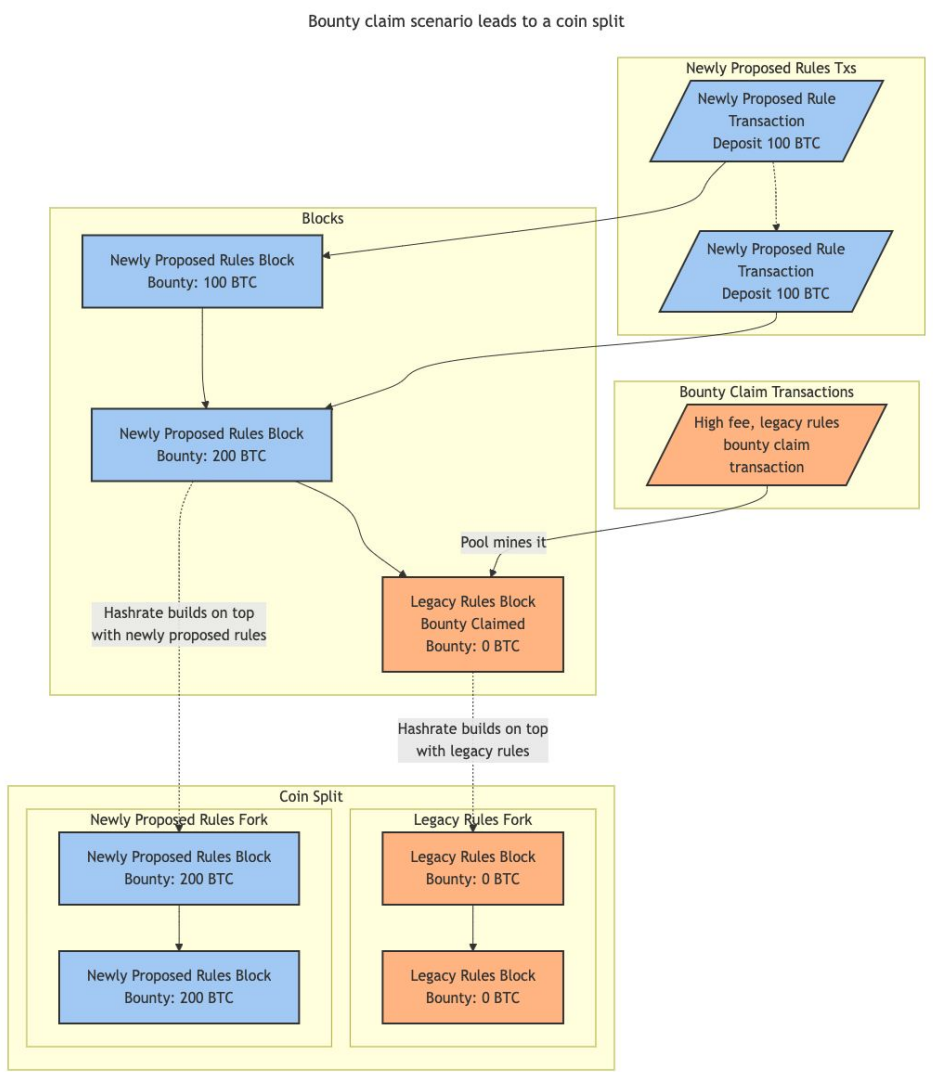
1. Passionate advocates for change becoming frustrated
2. Alternative clients created, marketed, and used
3. Miner activated soft forks that have weak Economic Node support result in brittle network at risk of chain splits

Soft fork consensus changes don’t require consensus to partially deploy and used but it creates a fragile network

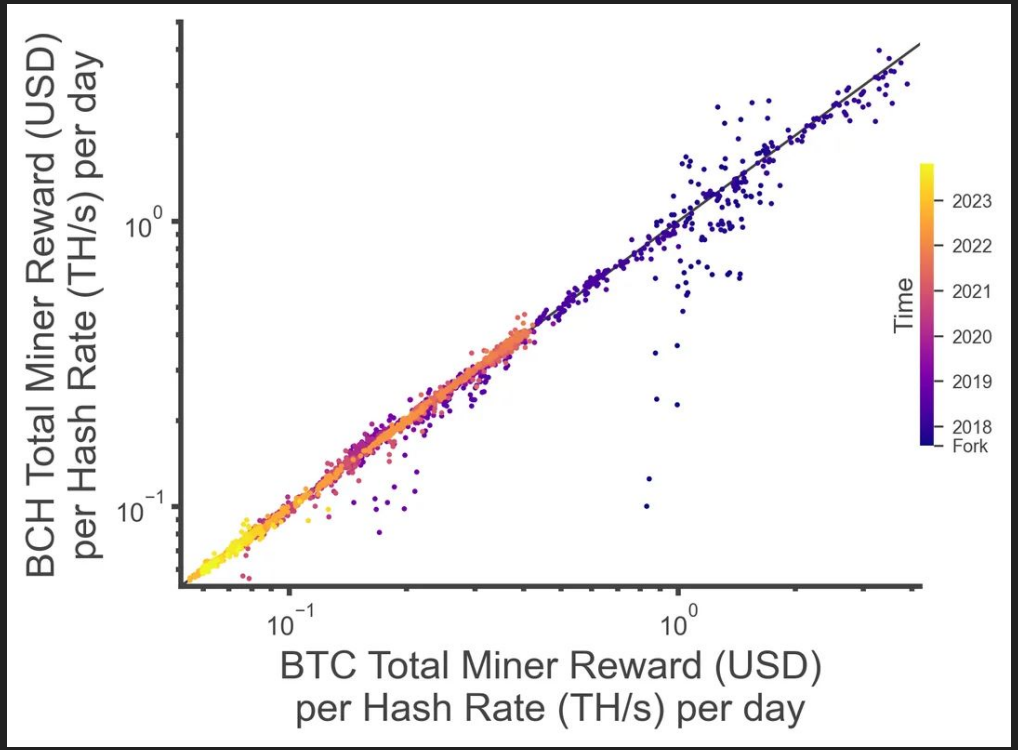


Bounty Claim Scenario

1. Fast moving apps, services, wallets offer users ability to lock btc in scripts based on consensus change that isn't widely adopted
2. Bounty is built up by these users of the Newly Proposed Rules
3. Anyone can claim the bounty with a single transaction and split the rewards as transaction fees with Miners
4. Risk is amplified when consensus change is rolled out with an Alternative Consensus Client because Economic Nodes need strong economic justification to switch from Bitcoin Core



Miners are economically motivated actors, Economic Nodes will list both coins and price will determine hashpower



Source: [Reddit, Coinmetrics]

Price is set at the margin, not all investors are equal

Segment of investor	Why they might support the legacy rules (Sell newly proposed rules coin)	Why they might support the newly proposed rules (Sell legacy rules coin)	Why they might be constrained from acting
Self custody, proprietary owner	Preference for stability and continuity with Protocol Developers	Actively building or investments in startups or applications that require the newly proposed rules	Unlikely to be constrained
Institutional Investors	Preference for stability and continuity with Protocol Developers	Investments in startups or applications that require the newly proposed rules	May be bound by contractual obligations or custodial limitations
Corporation with BTC on balance sheet	Preference for stability and continuity with Protocol Developers	Highly unlikely unless Protocol Developers no longer reflect the interests of other stakeholders	May require board or shareholder approval, slowing decision making
Exchange traded funds	Preference for stability and continuity with Protocol Developers	If their analysis suggests that the newly proposed rules could increase their assets under management	Their prospectus limits their ability to sell either coin, forcing them to choose and support only one

Takeaways

1. Six stakeholder groups with their own incentives and powers
2. Bitcoin Core maintainers do not have outsized power to change bitcoin, instead have outsized power to veto changes to bitcoin
3. Alternative client adoption is an important option but in practice very difficult to achieve
4. Soft fork consensus changes don’t require consensus to partially deploy and use, but create a fragile network prone to forking and uncertain outcomes
5. Not all investors are equal in price discovery during a hard fork, several larger investor segments are likely to react slower if at all
6. Stakeholder States of Minds impacts their influence on consensus
7. Investors don’t run economic nodes, their power is diminished until there is a chain split or futures market

Contributions welcome!

github.com/bitcoin-cap/bcap

Thank you:

Mat Balez, Jay Beddict, Jeff Booth, Joe Carlasare, John Carvalho, Hong Fang, David Harding, Avichal Garg, Gwart, Chaitanya Jain, Shirish Jajodia, Adam Jonas, Hong Kim, David King, Jameson Lopp, Shehzan Maredia, Sanjay Mavinkurve, Murch, Matt Odell, John Pfeffer, Reardencode, Bradley Rettler, Rijndael, Pierre Rochard, AJ Towns, Leo Wandersleb, 0xkrane, jesmros