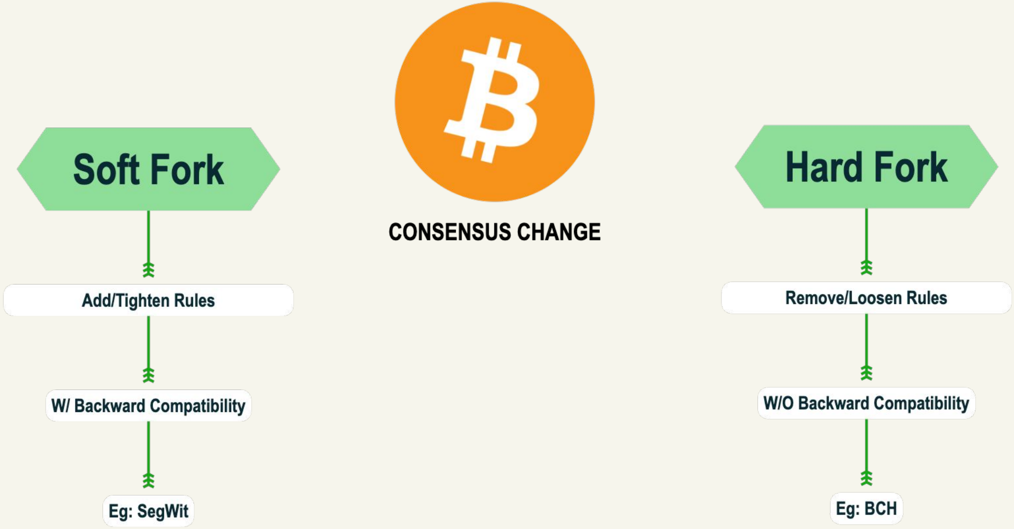
A Brief Report On Bitcoin's Next Upgrade For All

Kevin He,
Co-Founder @BitlayerLabs

Bitcoin Upgrade: What and Why

- When talking about [Bitcoin Upgrades], people generally means **consensus** [Hard Fork] or **[Soft Fork]**, mostly the latter



https://github.com/bitcoin/bips/blob/master/bip-0123.mediawiki

Bitcoin Upgrade: What and Why

- Reasons for an upgrade include: **Sustainability** and **Adaptability**

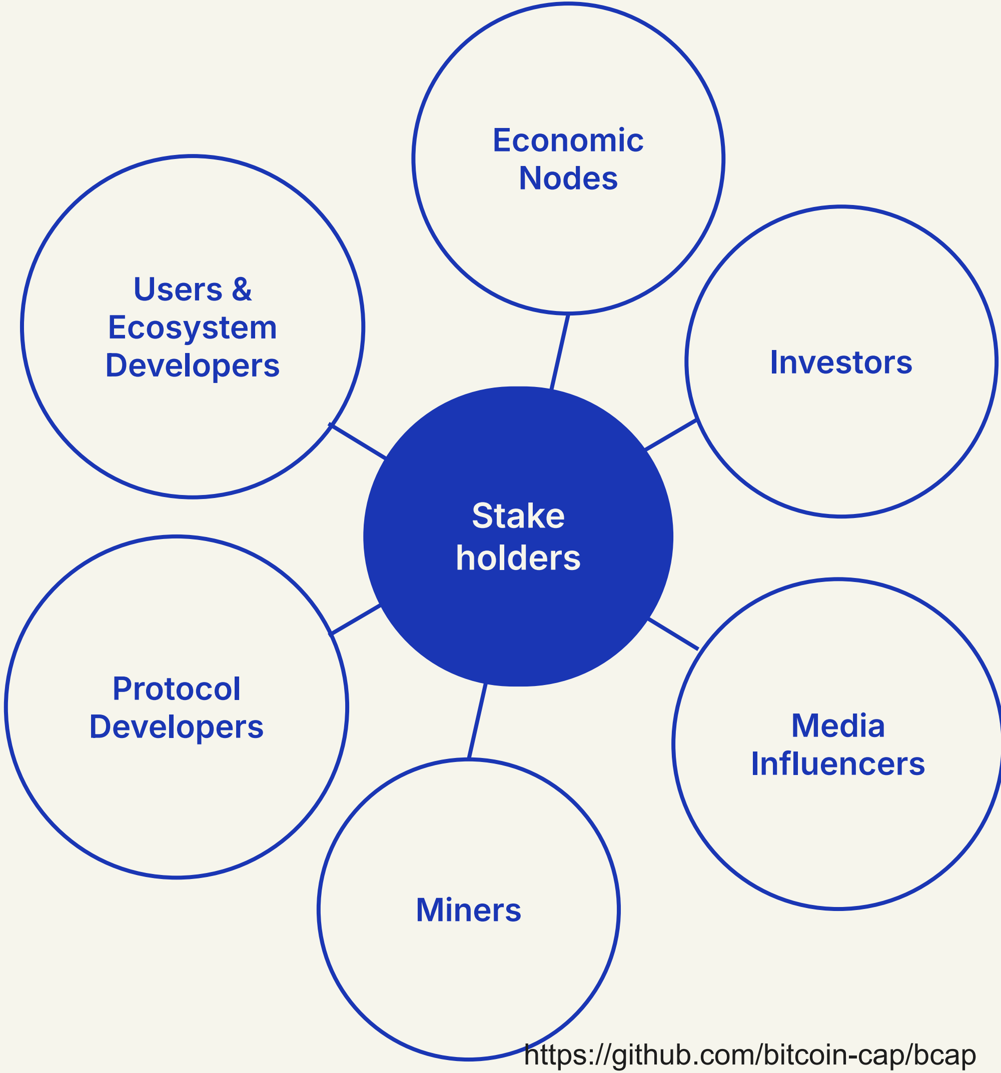
CONSENSUS CHANGE

Consensus Change	Change	Unchanged
Pros	• Technological Advancement • Enhanced Security • Expanded Use Cases	• Stability and Trust • Avoids Split Risks • Minimizes Attack Surface
Cons	• Risk of Forking • Increased Complexity	• Technological Stagnation • Lacks Flexibility for New Demands

Stakeholders Analysis

Takeaways:

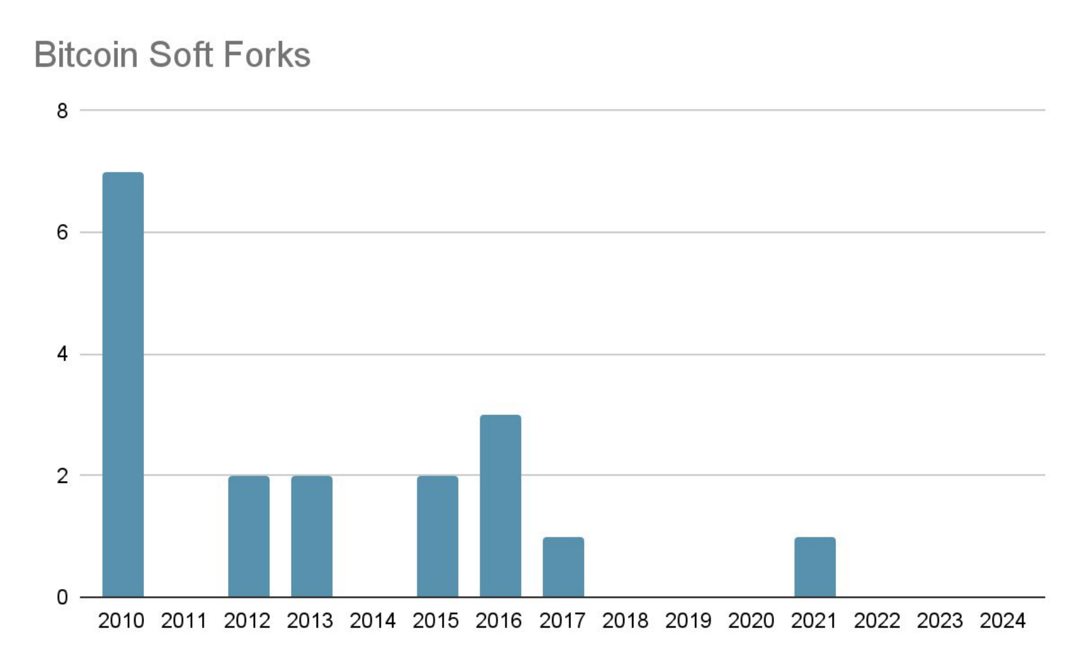
- Different stakeholders group with their own incentives and powers
- Protocol developers (the Core) have oversized power to veto changes
- Ecosystem developers support their favorable proposals



https://github.com/bitcoin-cap/bcap

History and Facts

- Less soft forks over time
- Longer time to reach consensus
- Community diversified



https://blog.bitmex.com/a-complete-history-of-bitcoins-consensus-forks-2022-update/
https://www.drivechain.info/media/slides/mit-2023.pdf

Previous Soft Forks Focus

Scalability

SegWit/Schnorr

Enhancing Bitcoin’s transaction capacity and efficiency to handle higher transaction volumes without increasing block size

Privacy

Taproot/MAST

Improving transaction privacy to obscure transaction types and protect user confidentiality on-chain

Programmability

CLTV/Tapscript

Expanding Bitcoin script functionality to support complex payment conditions and contracts, like delayed or conditional payments

Security

Disable Opcodes

Strengthening Bitcoin’s resilience against censorship and optimizing consensus activation mechanisms to maintain network security and decentralization.

A Good Soft Fork: The Sweet Spot

Potential/
Risk/
Position

Most people like it

No strong opposition

Change
Size

Not too simple

Nor too complex

Timing

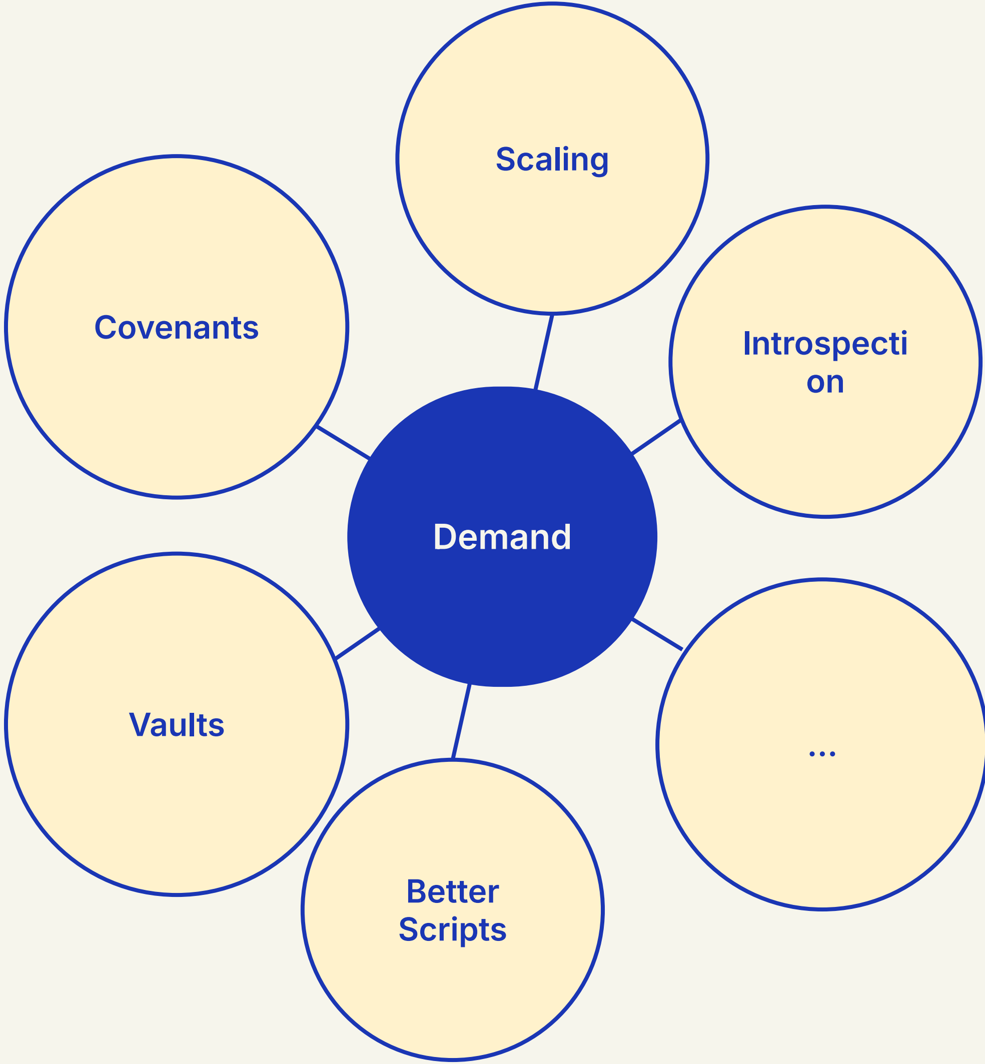
Strong Demand

Solve problems

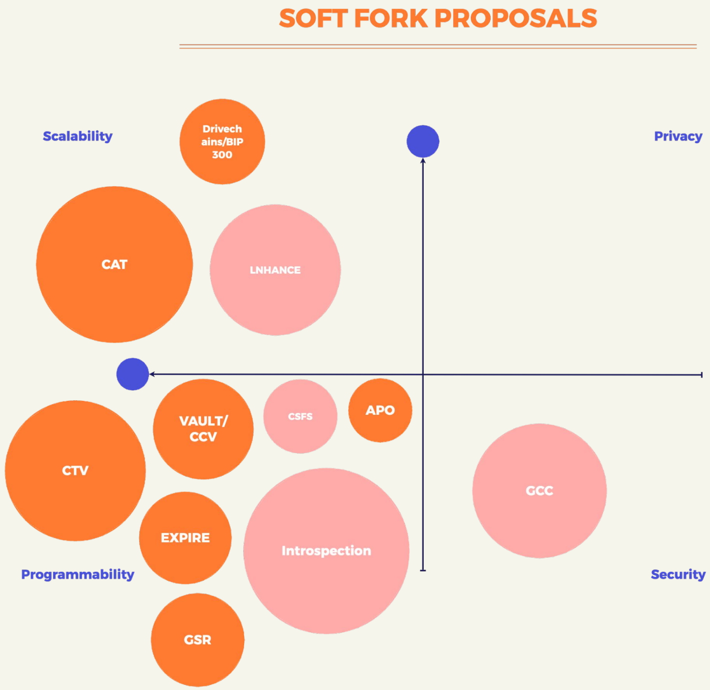
Community Voices

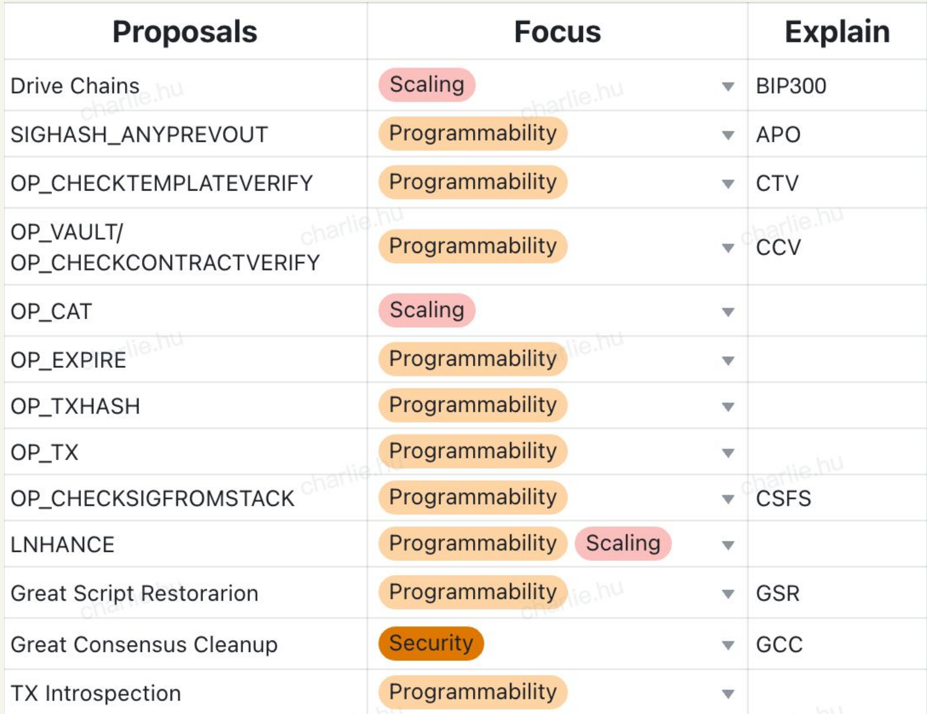
Focus:

- Conditional payments
- L2 Scaling
- ...



Next Soft Fork Proposals


SOFT FORK PROPOSALS


Proposals	Focus	Explain
Drive Chains	Scaling ▾	BIP300
SIGHASH_ANYPREVOUT	Programmability ▾	APO
OP_CHECKTEMPLATEVERIFY	Programmability ▾	CTV
OP_VAULT/ OP_CHECKCONTRACTVERIFY	Programmability ▾	CCV
OP_CAT	Scaling ▾	
OP_EXPIRE	Programmability ▾	
OP_TXHASH	Programmability ▾	
OP_TX	Programmability ▾	
OP_CHECKSIGFROMSTACK	Programmability ▾	CSFS
LNHANCE	Programmability Scaling ▾	
Great Script Restorarion	Programmability ▾	GSR
Great Consensus Cleanup	Security ▾	GCC
TX Introspection	Programmability ▾	

Consensus Maze

Too Huge to Change

$2T FDV, Most parties tend to remain stable

Core’s Role

Drafting, not sponsoring

Soft Fork Activation

Controversy about soft fork activation process

Governance

How about offchain voting

Urgency

No compelling reason to take the risk

Mass Stakeholders

Including governments

Takeaways

1. Changes are needed, soft fork is prefered
2. A good soft fork wins consensus fast
3. Stakeholders tend to be conservative
4. Any changes should preserve Bitcoin’s core value
5. Scaling is only one reason for upgrade
6. Good timing is needed
7. Better governance mechanism is needed