User Activated Soft Fork

Bitcoin scaling panel
The Israeli Bitcoin emBassy, 20 April 2017

Nadav Ivgi, Bitrated
nadav@bitrated.com

Quick recap: fork types

Soft fork

- Protocol *upgrade* mechanism
- Adds rules or tightens them
- Old software *accepts* new blocks
- Forward compatible, OK not to upgrade

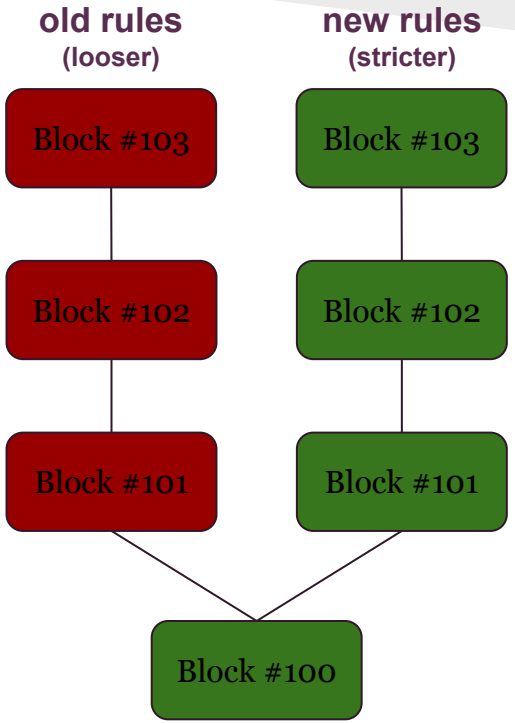
Hard fork

- Protocol *replacement* mechanism
- Removes rules or loosens them
- Old software *rejects* new blocks
- Not forward compatible, everyone has to upgrade

Distinction only comes into play if we account for non-upgraded nodes.
In a perfect world where everyone upgrades, none of this really matters.

Upgraded node PoV, soft-fork

Guaranteed to follow the right chain - it's the only one valid one.

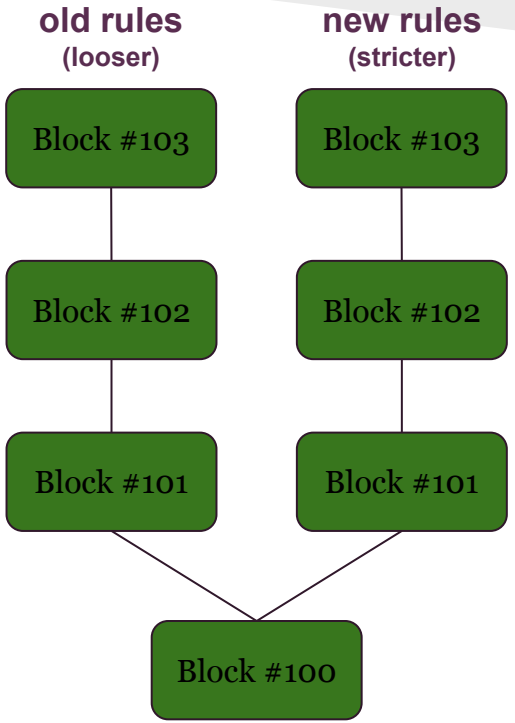


Non-upgraded PoV, soft-fork

Sees two valid chains, will follow the most-work one.

If the invalid (according to the stricter rules) chain is longer, we get a split between upgraded and non-upgraded nodes.

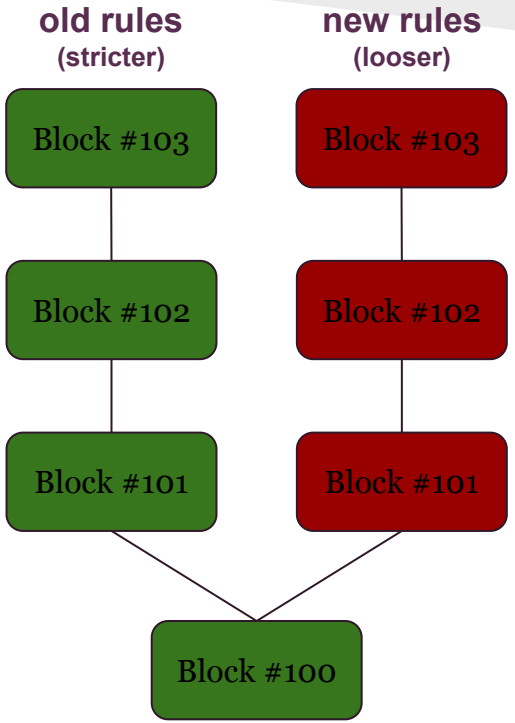
If the stricter-rules chain overtakes the invalid one, non-upgraded nodes will “hop” back to it and end the split.



Non-upgraded PoV, hard-fork

Will never accept the new (looser rules) chain.

A permanent split between upgraded and non-upgraded nodes is guaranteed.



Miner-activated soft-fork

- Miners signal readiness, activation coordination happens on-chain
- Safety mechanism to help ensure the stricter-rules chain is longer
  (but not guarantee it - miners can cheat)
- Secondary role: a way to roughly gauge community consensus <- this is broken :-(

User-activated soft-fork

- New consensus rules are enforced by full nodes on flag-day
- Coordination and consensus is off-chain, no miner signaling
- Misbehaving miners gets their blocks rejected by upgraded software (but not by old software)
- Split *possible* as long as miners can maintain the invalid (according to the stricter rules) chain as the longest chain
- Economic incentives should ensure miners eventually stop breaking the new rules, *if the UASF is overwhelmingly supported by the economic majority*

There are *two types* of UASF

Traditional (P2SH-like) UASF

- New features (stricter rules) enabled on flag-day
- Miners not forced to include transactions with new features, only not to break the new rules
- Opt-in, non-coercive: passive miners are OK, new rules will not be broken by standard software (even if not upgraded)
- For SegWit: requires everyone to upgrade again

BIP148 UASF

"User-enforced miner-activated soft-fork" for SegWit

- On flag day, start rejecting blocks that aren't signaling for segwit
- Enforces a 95% MASF activation for current segwit deployments, no need to re-upgrade
- Passive miners lose income, more coercive
- Economic sanction against miners: "signal for segwit or we ain't buying your coins"

PGP fingerprint

FCF1 9B67 8665 62F0 8A43 AAD6 81F6 104C D0F1 50FC

Nadav Ivgi, Bitrated
nadav@bitrated.com