Bitcoin protocol upgrades

“Future Politics - decentralized consensus in bitcoin”
The Israeli Bitcoin emBassy, February 2017

Nadav Ivgi, Bitrated
nadav@bitrated.com

Talk overview

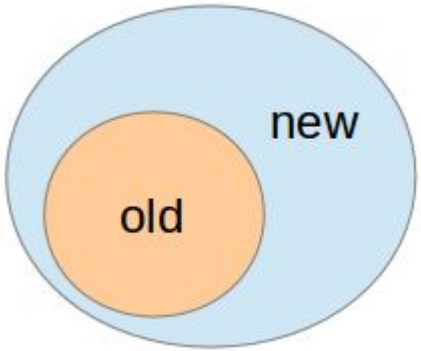
- Hard & soft forks
- Bitcoin Unlimited
- Segregated Witness

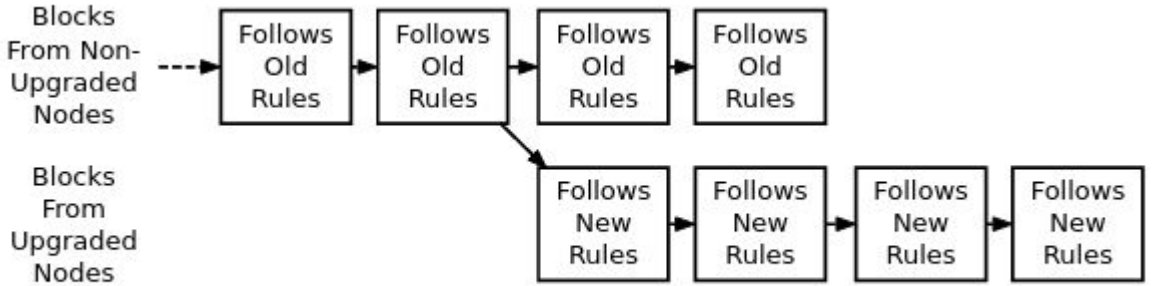
Hard forks

Protocol *replacement* mechanism based on on a coordinated network-wide upgrade

Hard forks

Can do *anything at all* (including removing rules) by making previously *invalid* blocks *valid*





A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Hard forks - the benefits

- Can do *anything*, very flexible
- Not caring about compatibility reduces software complexity
- Users explicitly opt-in to new protocol rules

Hard forks - criticism

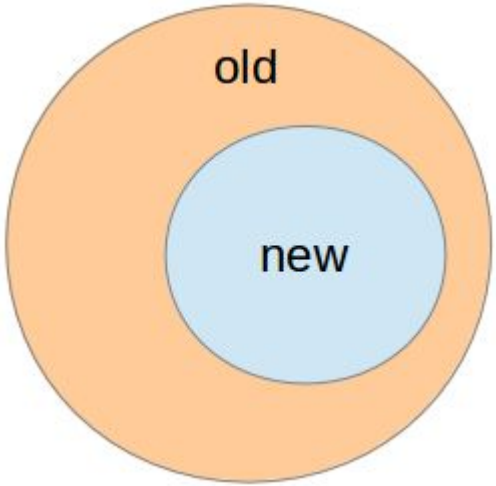
- Can do anything - bad precedent?
- Risks splitting the network and currency in two
- Non-upgraded nodes are broken and left open to attacks. Requires vigilance.
- Never done before, no past experience
- Slow to activate safely (months to years)

Soft forks

Protocol *upgrade* mechanism based on miner enforcement

Soft forks

Adds new protocol rules (but can't loosen them)
by making previously *valid* blocks *invalid*



Soft forks - the benefits

- Backward- and forward- compatible
- No currency split risk
- No disruption to users, everyone can upgrade at their leisure
- Experience with past deployments (P2SH, CSV, BIP66...)
- Fast to activate safely (weeks)

Soft forks - criticism

- Limited to certain kind of changes
- The compatibility requirement adds complexity
- Security is somewhat reduced for non-upgraded nodes
- Users accept new protocol rules by default, can opt-out

To recap… soft vs hard

Soft fork

- Protocol *upgrade* mechanism
- Forward compatible
  - Limited in what it can do
  - OK not to upgrade
  - No currency split risk
- Opt-in by default, can opt-out
- Fast deployment

Hard fork

- Protocol *replacement* mechanism
- Not forward compatible
  - Can do anything
  - Everyone has to upgrade
  - Currency split risk
- Opt-out by default, can opt-in
- Slow deployment

Bitcoin Unlimited

Hard-fork upgrade to a dynamic block size determined via “emergent consensus”

Bitcoin Unlimited

- Removes the hard block-size limit entirely
- “Emergent consensus” mechanism to allow miners to coordinate block size
- Miner support: 21.5% (BTC.TOP, Bitcoin.com (Roger Ver), GBMiners and ViaBTC (*BITMAIN backed?*))
- Separate development team

BU - the benefits

- Capacity increase
- Long-term solution
- Hardfork-related benefits

BU - criticism

- Hardfork-related criticism (currency split, unsafe, slow)
- Puts more control at the hand of miners
- “Emergent consensus” is a radical change that is unproven, untested and not peer-reviewed
- Centralization effects due to larger blocks
- Security concerns relating to fee market
- Several known attack vectors still left unattended
  no replay attack protection, no activation threshold, no grace period, several known hashpower-splitting vulnerabilities (*“0.6% attack”*)

Segregated Witness

Soft-fork upgrade to resolve malleability, increase capacity and more

Segregated Witness

- Originally developed to to resolve malleability, everything else is a bonus
- Activated with a 95% miner supermajority
- Miner support: 24% (Bitfury, BitClub and BTCC)
- Supported by over 100 businesses and projects
  tiny.cc/segwit-support
- Adopted by Litecoin, Stratis, Vertcoin, Viacoin and Groestlcoin

SegWit - the benefits

1. Fixes malleability, enabling a whole set of smart contracts
2. Doubles (+) the effective block size and network capacity
3. Security and efficiency gains for hardware wallets
4. New script versioning system to ease future upgrades
5. New hybrid security model between SPV and full node
6. Aligns cost incentives (bloating the UTXO is more expensive)
7. Resolves quadratic scaling time
8. Improves P2SH security to 256 bits

SegWit - criticism

- Softfork-related criticism (complexity, opt-out)
- One-time increase, not a long-term solution
- Centralization effects due to larger blocks
- Security concerns relating to fee market

nadav@bitrated.com

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