BIP99 and uncontroversial hardforks

Jorge Timón

December 5, 2015

Outline

Introduction

Uncontroversial consensus forks

Disagreements and controversial consensus forks

BIP99: Let's classify consenus forks

- Why?
- Common terminology
- Deployment recommendations
- Let's deploy an uncontroversial hardfork!

Softforks vs Hardforks

- Softfork: Everything that was invalid, is still invalid and more
  (backwards compatible for non-mining full nodes)
- Hardfork: Some previously-invalid blocks will be valid from now on
  (breaks backwards compatibility)

Unintentional consensus forks

- Accidents happen
- Softforks vs Hardforks?
- Deployment recommendation: **Do not deploy**
- What is the specification of the consensus rules anyway?

Specification (aka Libconsensus)

- Not this: https://en.bitcoin.it/wiki/Protocol_rules
- Current API: VerifyScript
- Future API?: VerifyHeader, VerifyTx, VerifyBlock
- Eventually its own repository?
- Specification and Implementation

Uncontroversial softforks

- Backwards compatible

  (infinite time to upgrade unless you want to use the new features)
- Successful precedents:
  - BIP30: #915 March 15th 2012 [block.nTime]
  - BIP16: #748 April 1st 2012 [block.nTime]
  - BIP34: #1526 March 25th 2013 (block 227931) [nHeight]
  - BIP66: #5713 July 4th 2015 [ISM v3]
  - BIP65: #6351 [Currently being deployed with ISM block version=4]
- Miners' upgrade confirmation (aka voting)
- Deployment recommendation: BIP9 (Version bits[specifically 29 of the 32 bits])

Uncontroversial hardfork: never too late for. . .

- Fix the "timewarp attack"
- Recovery of soft-fork bits from nVersion / reset the minimum version to 0 (unsigned)
- Increase of soft-fork NOP space.
- Recovery of low-order bits from CBlockHeader::hashPrevBlock
- . . .

Uncontroversial hardfork: deployment, let's do a hard fork asap!

- How long is "asap" and "long enough" at the same time? 1 year? 2 years? 5 years?
- Deployment recommendation: Minimum temporal threshold + BIP9
- Temporal threshold: header.nTime, block.nHeight, MedianTime(block.prev)

Controversial softfork

- Coordinated censorship
- Unpopular restriction
- Deployment recommendation: Please, miners, don't deploy

Schism hardfork deployment

- Don't care about miners opinion
- Deployment recommendation: only time threshold (no BIP9)
- Let's avoid hurt bystanders
- The first block in the fork should have a previously invalid nVersion

Schism hardfork examples

- Anti-Block-creator hardfork (without ASIC-reset)
- ASIC-reset hardfork
- Anti-cabal hardfork
- Spin-offs
- Differences in fundamental values

Disagreements and schism hardfork

- "People can disagree for unbounded amounts of time"
- Example: Some people disagree with this statement to date.

  Funny fact: until they agree, they represent a counter-example to falsify the opposite statement
- Do people have to follow the majority?
  - As shown by anti-ASIC hardforks, not the hashrate majority
  - The user's majority is not measurable
  - So called "economic majority" doesn't guarantee currency unification

Questions???

- jtimon@blockstream.com / jtimon@jtimon.cc
- Github, IRC: jtimon
- Twitter: @timoncc