

Bitcoin Changes — Soft Fork History and Theory

TabConf 2024

Oct 25, 2024

Paul Sztorc

Past TabConf Talks

Dec 2013 - Truthcoin
July 2015 – The Win-win
Blocksize solution,
Fork Futures via the
Exchange



TabConf 2018
Prediction Markets /
Futarchy



- Augur/Gnosis (MM 2014/2015)
- Polymarket (>\$1.5B last month)
- Solana (Meta-DAO), \$75 M

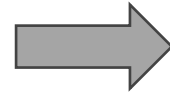
"This is something that could entirely reshape human civilization," Proph3t said. "This could solve politics."



May 2016 -Sidechain
Privatization
Jan 2017 - Blind
Merged Mining



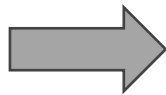
TabConf 2019
"Sidechain leeching"



- "MEV" (\$m/day)
- Producer-Builder separation



Nov 2015 -
Drivechain



TabConf 2021 - Drivechain
2023 - Debate with Peter

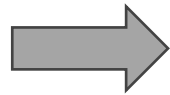


- Eigenlayer (\$100M a16z)
- Planetary scale (\$X00 B/yr)
 - zCash-privacy
- Eternal competitiveness
- ...



Dec 2016

"Better Fork Terminology"
"Against the Hard fork"
"Forks and Splits" (later)



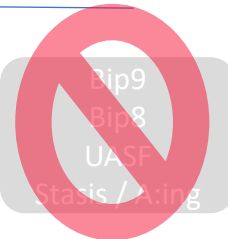
MIT Talk
2023
Softforks



CUSF
2024



Today's
Talk



Agenda

Intro	5 minutes
Soft Fork Basics & History	10 minutes
Soft Forks & Protocol Governance	10 minutes
Soft Forks Over Time	5 minutes
CUSF	5 minutes
Q&A	10 minutes

One Slide About Me

- Author BIPs 300/301 “Drivechain” – drivechain.info
- Bitcoin Researcher and Blogger – truthcoin.info
- Founder LayerTwo Labs – LayerTwoLabs.com
 - “making every transaction a Bitcoin txn”
 - SigNet Testnet , + faucet + explorer
 - CUSF Bip300/301 Activator for Core .. (+ OP_CAT also)
 - Zk-snark L2 (“Zcash sidechain”)
 - EVM-L2 (“EthSide”)
 - BitNames – Namecoin L2
 - BitAssets – Counterparty/Ordinals/Erc20 L2
 - Thunder – set of largeblock sidechains
 - New GUI for Bitcoin Core
- Fmr Statistician in the Yale Econ Department (2012-2015)

My Opinion



Waste of Time
(no offense)

Soft Forks

Basics/History

Part 1 of 4

Soft Forks – The Basics

- Soft vs Hard
 - “Tighten Rules” vs “Loosen Rules”
 - Optional Discretionary Upgrade vs Immediate Mandatory Upgrade
- Notable Soft Forks
 - Aug 2010 – Disable a bunch of opcodes
 - Sep 2010 – Limit blocksize to 1 MB
 - Apr 2012 – Add P2SH
 - Dec 2015 – Add CLTV
 - Aug 2017 – Add SegWit
- Infamous Attempted Hard Forks
 - 2015 – Raise the Blocksize Limit (BitcoinXT / Bitcoin Classic / etc)
 - 2017 – SegWit2x
 - 2017 – BCH (which became its own community)

Some History – Not Widely Known

1. Gavin Called Them “Soft **Changes**” (June 2012)
2. “Changes” is a better term – “Fork” is a bad term.
3. How the “Soft Fork” Term created (Nov 2012)
 1. And why it’s actually good.
4. The Logic Behind It All

Gavin Called them “Soft Changes”



gavinandresen / BitcoinVersioning.md

Created 11 years ago

<> Code

Revisions 5

Stars 11

Forks 7

Embed ▾

Revisions

Split

Unified



gavinandresen revised this gist on Jun 29, 2012.

1 changed file with 4 additions and 0 deletions.

4 BitcoinVersioning.md



@@ -2,6 +2,10 @@

2 2

3 3

We recently rolled out two changes to the Bitcoin block acceptance rules (BIP16 and BIP30); this document records the lessons learned and makes recommendations for handling future blockchain rule changes.

4 4

+ Note: there are "soft" rule changes and "hard" rule changes. "Soft" changes tighten up the rules-- old software will accept all the blocks and transactions created by new software, but the opposite may not be true. "Soft" changes do not require the entire network of miners and merchants and users to upgrade or be left behind.

6 +

7 +

"Hard" changes modify the rules in a way that old, un-upgraded software consider illegal. At this point it is much, much more difficult (some might say impossible) to roll out "hard" changes, because they require every miner and merchant and user to upgrade.

8 +

5 9

Lessons Learned

6 10

7 11

+ Be sure to consider all 4 combinations of old/new software running before/after the majority of the network supports the new rule(s).

Gavin Called them "Soft Changes"



gavinandresen / BitcoinVersioning.md

Created 11 years ago

<> Code

Revisions 5

Stars 11

Forks 7

Embed

Revisions

Split

Unified



gavinandresen revised this gist on Jun 29, 2012.

1 changed file with 4 additions and 0 deletions.

4 BitcoinVersioning.md

@@ -2,6 +2,10 @@

2 2

3 3

We recently rolled out two changes to the Bitcoin block acceptance rules (BIP16 and BIP30); this document records the lessons learned and makes recommendations for handling future blockchain rule changes.

4 4

+ Note: there are "soft" rule changes and "hard" rule changes. "Soft" changes tighten up the rules-- old software will accept all the blocks and transactions created by new software, but the opposite may not be true. "Soft" changes do not require the entire network of miners and merchants and users to upgrade or be left behind.

6 +

+ "Hard" changes modify the rules in a way that old, un-upgraded software consider illegal. At this point it is much, much more difficult (some might say impossible) to roll out "hard" changes, because they require every miner and merchant and user to upgrade.

Lessons Learned

7 11

+ Be sure to consider all 4 combinations of old/new software running before/after the majority of the network supports the new rule(s).

Forbidden, on grounds of impracticality

In Blockchain, Fork Has a Strange Meaning

Culinary Fork?



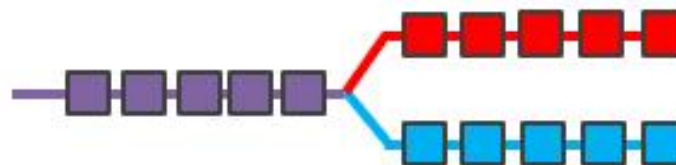
Tuning Fork?



Fork in the
Road?



Blockchain
(hard/soft) Fork?



...at least, not if you ask me!

Welcome, **Guest**. Please [login](#) or [register](#).

News: Latest Bitcoin Core release: [24.0.1](#) [[Torrent](#)]

[HOME](#)

[HELP](#)

[SEARCH](#)

[LOGIN](#)

[REGISTER](#)

[MORE](#)

Nov 2012 – Definitions

[Bitcoin Forum](#) > [Other](#) > [Beginners & Help](#) > [Terminology](#)

Pages: [[1](#)] [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#) [37](#) [38](#) [39](#) [40](#) [41](#) »



Author

Topic: Terminology (Read 79459 times)

yogi (OP)

Legendary



Activity: 947

Merit: 1038



Hamster ate my bitcoin



Terminology



November 19, 2012, 10:58:51 PM

Merited by [Ryan Dugan](#) (10), [suchmoon](#) (4), [hugeblack](#) (4), [BTCforJoe](#) (4), [vapourminer](#) (3), [Quickseller](#) (3), [In](#) (1), [xtraelv](#) (1), [HabBear](#) (1), [butka](#) (1), [BlackBoss_](#) (1), [Saruman](#) (1), [Crypto-DesignService](#) (1)

Terminology

Commonly used abbreviations, words, names and phrases on bitcointalk.

Sections

[BITCOINTALK](#)

[BITCOIN](#)

[PEOPLE](#)

[PLACES](#)

[ALTCOINS](#)

Nov 2012 – Definitions

'Fork'

- 1) See - 'Software Fork'.
- 2) See - 'Soft Fork'.
- 3) See - 'Hard Fork'.

'Hard Fork'

When there are a sufficient number of bitcoin clients on the network that disagree on the rules about how blocks are created and recorded in the blockchain. It leads to a split in the chain, one set of bitcoin clients follow one branch and another set follows the other. To fix **hard forks** some action must be taken by us.

'Online Wallet'

See - 'Browser Based Wallet'

'Orphaned Blocks'


Whenever a **Soft Fork** or 'Hard Fork' occurs, the blockchain is split into two paths. One of these chains will eventually be considered the valid one, and the other will be the invalid chain. Block that are in an invalid chain are called orphaned blocks.


'Paper Wallet'

'Soft Fork'

- 1) A situation where two or more competing blocks are published at the same height in the blockchain. These kinds of forks will solve themselves without any intervention from us.
- 2) See - 'Software Fork'.



Even Adam
Back and Luke
Dashjr
Disagree


 **r/bitcoin** comments other discussions (1) show images (0)

 **soft fork for size increase?** (self.Bitcoin)
submitted 1 day ago by [frank01945](#)

Is there a technical reason why a blocksize increase cannot be done via a soft fork after segwit?

10 comments source share save hide give gold report hide all child comments

[+] adam3us  **3 points** 1 day ago* (last edited 17 hours ago)



Yes you can increase size via soft-fork see https://www.reddit.com/r/Bitcoin/comments/39kqzs/how_about_a_softfork_optin_blocksize_increase using extension blocks.


In some ways segwit itself is a simplified extension block, and does some of the work towards enabling extension-blockss.

Like segwit an ext-block is opt-in and forwards and backwards compatible.

Note it is not without downsides because it does increase block size and can be done via soft fork, where a hard fork requires more agreement from users, investors, exchanges etc.



permalink source embed save save-RES report give gold reply hide child comments


 


[+] luke-jr  **1 point** 18 hours ago



Extension blocks are not a softfork.


permalink source embed save save-RES parent report give gold reply

[+] adam3us  **1 point** (0 children)



[+] jcoiner  **2 points** 1 day ago (3 children)


 

[+] frank01945  **[S] 2 points** 1 day ago

I just found Peter's remarks: <https://petertodd.org/2016/forced-soft-forks>



permalink source embed save save-RES report give gold reply hide child comments


 

[+] luke-jr  **2 points** 18 hours ago

He's really describing a hardfork there, though.

permalink source embed save save-RES parent report give gold reply

[+] adam3us  **2 points** 15 hours ago

Yes [/u/petertodd](#) is talking about a soft-hardfork there, which has also been called a firm-fork or evil-fork. The BIP [/u/luke-jr](#) and [/u/jl_2012](#) have been working on is one of these kinds of forks. I think this kind of fork is more hard than soft, in the sense that users basically have to upgrade (or fork away).

An extension-block is more soft-fork like because it is opt-in, and forwards and backwards compatible for users.

permalink source embed save save-RES parent report give gold reply



Nov 2012 – Definitions

'Fork'

- 1) See - 'Software Fork'.
- 2) See - 'Soft Fork'.
- 3) See - 'Hard Fork'.

'Hard Fork'

When there are a sufficient number of bitcoin clients on the network that disagree on the rules about how blocks are created and recorded in the blockchain. It leads to a split in the chain, one set of bitcoin clients follow one branch and another set follows the other. To fix **hard forks** some action must be taken by us.

'Online Wallet'

See - 'Browser Based Wallet'

'Orphaned Blocks'

Whenever a **Soft Fork** or 'Hard Fork' occurs, the blockchain is split into two paths. One of these chains will eventually be considered the valid one, and the other will be the invalid chain. Block that are in an invalid chain are called orphaned blocks.

'Paper Wallet'

'Soft Fork'

- 1) A situation where two or more competing blocks are published at the same height in the blockchain. These kinds of forks will solve themselves without any intervention from us.
- 2) See - 'Software Fork'.

The Logic (historic)

- A soft fork “will resolve itself”.
 - It will either collapse in the “use the new feature” direction, or...
 - ... it will collapse in the “new feature is broken” direction.
- If >50% hashrate upgrades to support a feature, then the fork will always resolve in the direction that supports the feature.
 - Rebel-blocks are always orphaned (it is as if they arrived too late).
 - Thus, a feature goes from being 0% safe, to 100% safe, on a defined date.
 - With hashrate-signaling, everyone can learn the exact date that the feature activates.
- Very useful!
 - ...paired with “blank” anyone-can-spend OP NOP

A concise soft fork

Summary

CHECKLOCKTIMEVERIFY redefines the existing NOP2 opcode. When executed, if any of the following conditions are true, the script interpreter will terminate with an error:

- the stack is empty; or
- the top item on the stack is less than 0; or
- the lock-time type (height vs. timestamp) of the top stack item and the nLockTime field are not the same; or
- the top stack item is greater than the transaction's nLockTime field; or
- the nSequence field of the txin is 0xffffffff;

Otherwise, script execution will continue as if a NOP had been executed.

Default behavior = allow the txn

Soft Forks and Protocol Governance

Part 2 of 4

Governance – Definition



The screenshot shows the Merriam-Webster website interface. At the top, there is a dark blue navigation bar with the Merriam-Webster logo on the left, which includes the text "Merriam-Webster" and "Est. 1828". To the right of the logo are two red buttons labeled "Dictionary" and "Thesaurus". Further right is a search bar containing the word "governance" with a red search button. To the right of the search bar are links for "Games & Quizzes", "Thesaurus", "Features", and "Word Finder".

On the left side of the page, there is a dark blue sidebar with a red banner labeled "Definition". Below this banner are links for "Synonyms", "Example Sentences", "Word History", and "Phrases Containing".

The main content area displays the word "governance" in a large, bold, serif font, followed by the word "noun" in a smaller, blue, sans-serif font. Below this, the word is written in a smaller, lowercase, sans-serif font as "gov·er·nance", followed by a pronunciation guide in a rounded rectangle: "'gə-vər-nən(t)s" with a speaker icon. Below the pronunciation guide is the word "plural" in a light blue box, followed by "governances" in a bold, sans-serif font. Below this is a link for "Synonyms of governance" in a blue, sans-serif font. The definition itself is written in a serif font: ": the act or process of governing or overseeing the control and direction of something (such as a country or an organization) : GOVERNMENT".

Governance – Definition



The screenshot shows the Merriam-Webster website interface. At the top, there is a navigation bar with links for 'Dictionary', 'Thesaurus', 'Games & Quizzes', 'Thesaurus', 'Features', and 'Word Finder'. The search bar contains the word 'governance' and a magnifying glass icon. On the left side, there is a sidebar with the Merriam-Webster logo, 'Est. 1828', and the word 'Dictionary'. Below this, there are links for 'Definition', 'Synonyms', 'Example Sentences', 'Word History', and 'Phrases Containing'. The main content area displays the word 'governance' in a large, bold font, followed by the word 'noun'. Below this, there is a pronunciation guide: 'gov·er·nance' and a phonetic transcription 'gə-vər-nən(t)s' with a speaker icon. There is also a link for 'plural governances' and a link for 'Synonyms of governance >'. The definition is provided in a large font: ': the act or process of governing or overseeing the control and direction of something (such as a country or an organization) : GOVERNMENT'. Below the definition, there is a partially visible sentence: '...a controlled system of governance'.

Merriam-Webster
Est. 1828
Dictionary

Dictionary Thesaurus

governance

Games & Quizzes Thesaurus Features Word Finder

governance noun

gov·er·nance 'gə-vər-nən(t)s

plural **governances**

[Synonyms of governance >](#)

: the act or process of **governing** or overseeing the control and direction of something (such as a country or an organization) : **GOVERNMENT**

...a controlled system of governance

- Rejects P2P

Governance – Definition



The screenshot shows the Merriam-Webster website interface. At the top, there is a navigation bar with links for 'Dictionary', 'Thesaurus', 'Games & Quizzes', 'Thesaurus', 'Features', and 'Word Finder'. The search bar contains the word 'governance'. On the left side, there is a sidebar with a 'Definition' tab highlighted in red, and other tabs for 'Synonyms', 'Example Sentences', 'Word History', and 'Phrases Containing'. The main content area displays the word 'governance' as a noun, with its phonetic transcription 'gov·er·nance' and 'gə-vər-nən(t)s'. It also shows the plural form 'governances' and a link to 'Synonyms of governance'. The definition provided is: 'the act or process of governing or overseeing the control and direction of something (such as a country or an organization) : GOVERNMENT'.

Merriam-Webster
Est. 1828
Dictionary

Definition

Synonyms
Example Sentences
Word History
Phrases Containing

governance noun

gov·er·nance 'gə-vər-nən(t)s

plural **governances**

[Synonyms of governance >](#)

: the act or process of **governing** or overseeing the control and direction of something (such as a country or an organization) : **GOVERNMENT**

- Rejects P2P
- Too vague!! (There is no success criterion, no objective function.)

Governance = Finding today's node software

- Governance = where does the node software come from? What process?
- In that sense, it is more like an industrial process, or recipe.
(Eg, how do we build a bridge? How do we build the node software?)
 - Which code is fullnode-code?
 - How do we tell Bitcoin Nodes from non-nodes?
 - If there is a dispute, then who is correct (and who is wrong)? Why?
- In other words, Governance is:
 - The problem of meta-consensus ; consensus about consensus.
(A full node does consensus, but only after you find the node software and run it!)
 - Or, call it “pre-consensus”. How do find the consensus software.
 - If you didn't have a node, how would you get one?

Governance

Problem: What is today's node software ? → I know how to find it!

- I will call this: “Node Constructor-Theory”

NodeFinding Strategies – The Big 3

1. Go to Bitcoin.org and Run The Latest Version

1. Luke Dashjr Position
2. Mike Hearn position as well!
3. Satoshi's position, (?) repudiated when he removed OP VER.

2. Find the oldest node-like thing, run that, then plug your ears!

1. Never revisit this process. The relative costs and benefits – the node software does consensus pretty well, meta-consensus is much harder to do. Be mistrustful of this.
2. Mircea Popescu's "Bitcoin Foundation" – 0.5.4 (2014)
3. The "original" is the full node. Everything later is a *distortion*. Everything afterwards is ...wargames for a bait-and-switch.

3. Soft Fork "Pluralism"

1. Soft fork means that different pieces of software can coexist
2. Anything in the "Line of Coexistence" is fair game!

"Latest
Core"

"Static"
Protocol

"Linear
Coexistence"
(Consent-
Based)

Mike Hearn

OK, so your node has rejected a block because it didn't understand it. Now what? In our imaginary firm the auditors would call the CEO (you) and ask for a decision. You're The Decider™. And so it is with Bitcoin: you will be alerted in some way, like via SMS or email if you configured that, and you get to decide what to do. You could ...

1. Read about the rule change and decide that you're OK with it. Upgrade and continue.
2. Read about the rule change and decide you're **not** OK with it. More on this in a second.
3. Explicitly decide to trust any spend of the scripts you don't understand. You might do this if uptime of your node is more important to you than correct audit results.

The last option is risky but hey, check it out — you just got the soft forking behaviour back! The difference is, you explicitly requested it and your choice doesn't affect anyone else. Only you take the risk of calculating an incorrect ledger. Bitcoin Core & XT don't support the third option today, but adding a switch to enable it would be easy if anyone wanted that.

<https://medium.com/@octskyward/on-consensus-and-forks-c6a050c792e7>

Satoshi – OP VER

- ▲ Given OP_VER (0x62) was never used onchain, is disabled and is not considered useful can its meaning be stripped and it be made OP_SUCCESS for the purposes of introducing a new different opcode in future?
- 2
- ▼ As Andrew Poelstra [describes](#) "...there was an opcode called OP_VER, OP version. I can see some grimaces. It would push the client version onto the stack. This meant that when you upgraded Bitcoin say from 0.1 to 0.2, that's a hard fork. Now script will execute OP_VER and push 0.1 onto the stack for some people and 0.2 onto the stack for other people. You've forked your chain. Fortunately nobody ever used this opcode which is good."

[script](#) [bitcoin-core-development](#) [taproot](#) [opcodes](#)

Share Improve this question Follow

edited Oct 26, 2020 at 0:03

asked Jul 29, 2020 at 10:48

 Michael Folkson
12.8k ● 3 ● 10 ● 38

BIP342 does in fact turn it into an OP_SUCCESS. Is that a sufficient answer? – Pieter Wuille Jul 29, 2020 at 17:50

BIP 342 doesn't refer to 0x62 though...? Unless my BIP foo is off... – Michael Folkson Jul 29, 2020 at 18:12

1 Doh it is. I just can't convert from hex :-/ – Michael Folkson Jul 29, 2020 at 18:19

Add a comment

2 Answers

Sorted by: Highest score (default) ▼

▲ [BIP 342](#) does exactly this. (Thanks Pieter)

<https://bitcoin.stackexchange.com/questions/97258/given-op-ver-was-never-used-is-disabled-and-not-considered-useful-can-its-meani>

NodeFinding Strategies – The Big 3

1. Go to Bitcoin.org and Run The Latest Version

1. Luke Dashjr Position
2. Mike Hearn position as well!
3. Satoshi's position, (?) repudiated when he removed OP VER.

2. Find the oldest node-like thing, run that, then plug your ears!

1. Never revisit this process. The relative costs and benefits – the node software does consensus pretty well, meta-consensus is much harder to do. Be mistrustful of this.
2. Mircea Popescu's "Bitcoin Foundation" – 0.5.4 (2014)
3. The "original" is the full node. Everything later is a *distortion*. Everything afterwards is ...wargames for a bait-and-switch.

3. Soft Fork "Pluralism"

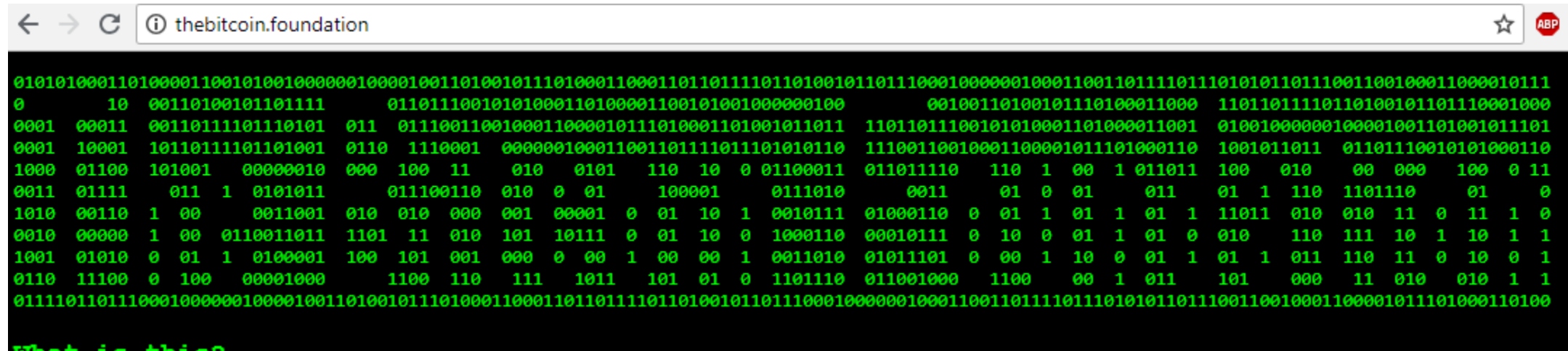
1. Soft fork means that different pieces of software can coexist
2. Anything in the "Line of Coexistence" is fair game!

"Latest
Core"

"Static"
Protocol

"Linear
Coexistence"
(Consent-
Based)

The “Static Protocol” Position



A screenshot of a web browser window displaying the Bitcoin Foundation website. The browser's address bar shows "thebitcoin.foundation". The page content is obscured by a dense, green, monospaced text overlay that resembles a mix of binary code and a legal disclaimer. The text is arranged in several horizontal lines across the page.

Archives:

(C) 2014 - 2018 The Bitcoin Foundation. You do not have, nor can you ever acquire the right to use, copy or distribute this software ; Should you use this software for any purpose, or copy and distribute it to anyone or in any manner, you are breaking the laws of whatever soi-disant jurisdiction, and you promise to continue doing so for the indefinite future. In any case, please always : read and understand any software ; verify any PGP signatures that you use - for any purpose.

- [0.5.4-RELEASE \[x86-64\] \[Latest\]](#): Build this with V, by following these steps
- [0.5.4-TEST2 \[x86-64\] \[Obsolete\] \[PGP Sig\]](#) SHA256: 6d37ec8b58cd5ec0ff5df71467a7d7cac684cfa517844e4d67a6611c9ae584ce
- [0.5.3.1-RELEASE \[Obsolete\]](#) SHA256: 5c41fe6cf286770a25bf61ab0c35747d0c760f8656754296d2e1d3c4274b5686
- [0.5.3 \[Origin Codebase - Obsolete\]](#) SHA256: aab1f8ea8c7f131ff69dfa3b9437ba35531018be760132dd6373f41a591f6382

- Bitcoin Foundation

NodeFinding Strategies – The Big 3

1. Go to Bitcoin.org and Run The Latest Version

1. Luke Dashjr Position
2. Mike Hearn position as well!
3. Satoshi's position, (?) repudiated when he removed OP VER.

2. Find the oldest node-like thing, run that, then plug your ears!

1. Never revisit this process. The relative costs and benefits – the node software does consensus pretty well, meta-consensus is much harder to do. Be mistrustful of this.
2. Mircea Popescu's "Bitcoin Foundation" – 0.5.4 (2014)
3. The "original" is the full node. Everything later is a *distortion*. Everything afterwards is ...wargames for a bait-and-switch.

3. Soft Fork "Pluralism"

1. Soft fork means that different pieces of software can coexist
2. Anything in the "Line of Coexistence" is fair game!

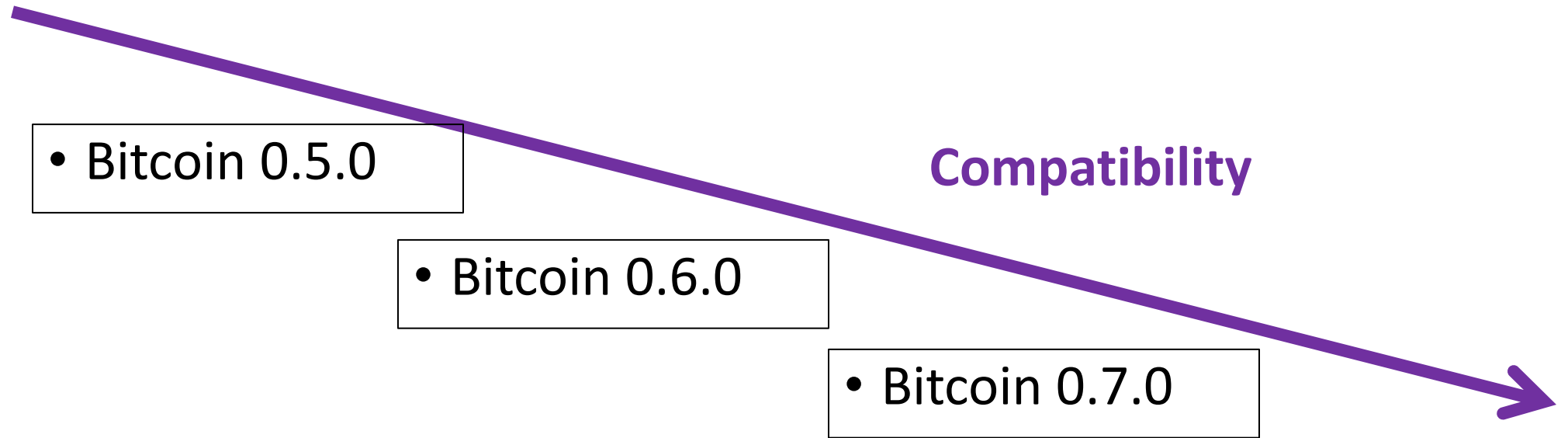
"Latest
Core"

"Static"
Protocol

"Linear
Coexistence"
(Consent-
Based)

Upgrading via Soft Fork

- “line” of protocols that are all compatible with each other



NodeFinding Strategies – The Big 3

1. Go to Bitcoin.org and Run The Latest Version

1. Luke Dashjr Position
2. Mike Hearn position as well!
3. Satoshi's position, (?) repudiated when he removed OP VER.

2. Find the oldest node-like thing, run that, then plug your ears!

1. Never revisit this process. The relative costs and benefits – the node software does consensus pretty well, meta-consensus is much harder to do. Be mistrustful of this.
2. Mircea Popescu's "Bitcoin Foundation" – 0.5.4 (2014)
3. The "original" is the full node. Everything later is a *distortion*. Everything afterwards is ...wargames for a bait-and-switch.

3. Soft Fork "Pluralism"

1. Soft fork means that different pieces of software can coexist
2. Anything in the "Line of Coexistence" is fair game!

"Latest
Core"

"Static"
Protocol

"Linear
Coexistence"
(Consent-
Based)

Governance Strategies... And their Problems

	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / “Dissent”
“Latest Core”			
“Static” Protocol			
“Linear Coexistence” (Consent- Based)			

Governance Strategies... And their Problems

	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / “Dissent”
“Latest Core”		Outsource Your Thinking to Bitcoin.org	
“Static” Protocol		Stays the Same	
“Linear Coexistence” (Consent-Based)			

Governance Strategies... And their Problems

	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / “Dissent”
“Latest Core”		Outsource Your Thinking to Bitcoin.org	
“Static” Protocol		Stays the Same	
“Linear Coexistence” (Consent-Based)		Allows Error-Correction	

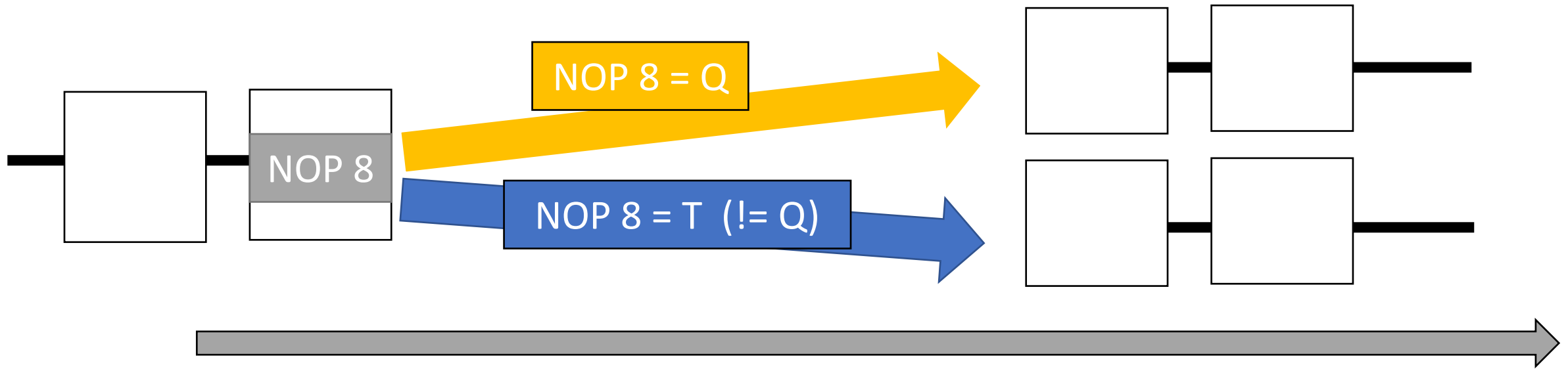
Expertise... is Mandatory!

- Luke-Jr Position:
 - Must run latest version. Running old versions of the software is illegitimate!
 - Must ensure the version on Bitcoin.org is good, by participating in technical community.
- Problems
 - Learning takes effort.
 - Impossible for everyone to be an expert!
 - Laypeople are important! But this view says: no laypeople allowed!
 - No accumulation of recognizability. Instead, continual effort needed.

Governance Strategies... And their Problems

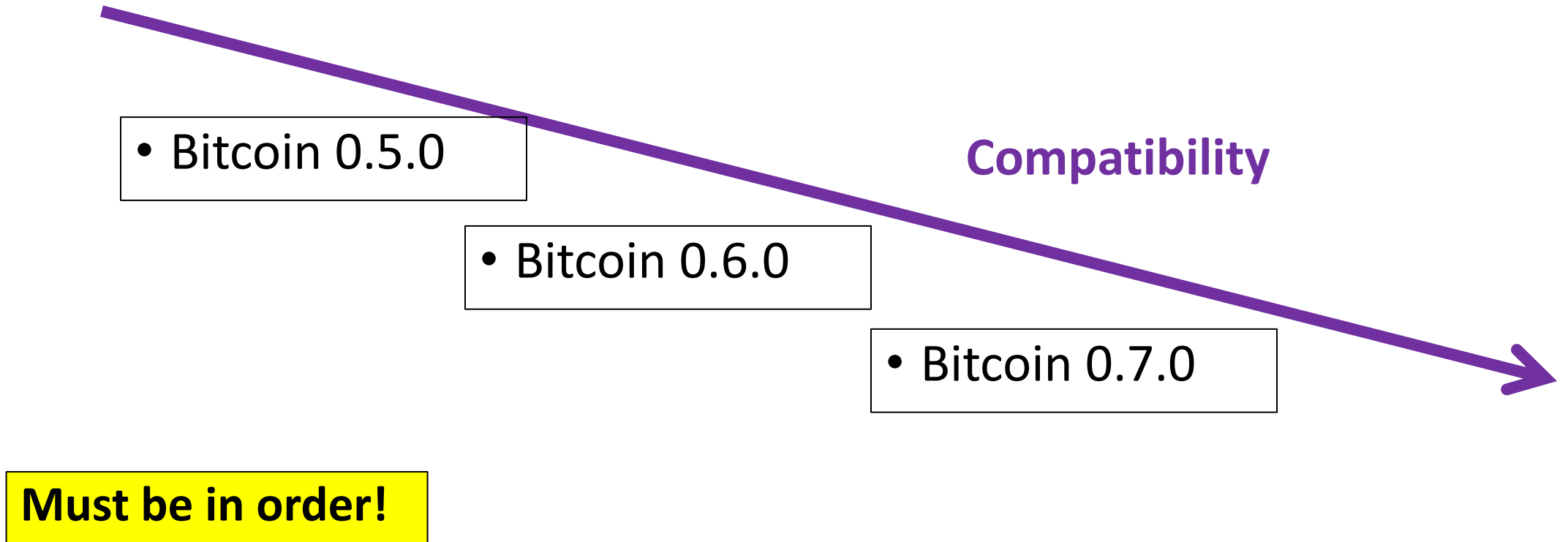
	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / “Dissent”
“Latest Core”	No Laypeople Allowed	Outsource Your Thinking to Bitcoin.org	
“Static” Protocol	Accumulates Trust	Stays the Same	
“Linear Coexistence” (Consent-Based)	Requires dispute-resolution	Allows Error-Correction	

Two Incompatible SFs at once = HF



Upgrading via Soft Fork

- “line” of protocols that are all compatible with each other



Bitcoiners Often Disagree

- Carnivores vs Vegans
- But also...
 - Bip9 vs Bip8
 - Lot=true vs false
 - Ordinals
 - US Regulation
 - Op Cat

...just about everything!



Governance Strategies... And their Problems

	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / "Dissent"
"Latest Core"	No Laypeople Allowed	Outsource Your Thinking to Bitcoin.org	
"Static" Protocol	Accumulates Trust	Stays the Same	
"Linear Coexistence" (Consent-Based)	Requires dispute-resolution	Allows Error-Correction	

Governance Strategies... And their Problems

	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / “Dissent”
“Latest Core”	No Laypeople Allowed	Outsource Your Thinking to Bitcoin.org	Allows Innovation
“Static” Protocol	Accumulates Trust	Stays the Same	No Innovation Allowed
“Linear Coexistence” (Consent-Based)	Requires dispute-resolution	“Ratchet” – Resists Future Errors	Allows Most Innovation

Governance Strategies... And their Problems

	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / “Dissent”
“Latest Core”	No Laypeople Allowed	Outsource Your Thinking to Bitcoin.org	Allows Innovation
“Static” Protocol	Accumulates Trust	Stays the Same	No Innovation Allowed
“Linear Coexistence” (Consent- Based)	Requires dispute- resolution	“Ratchet” – Resists Future Errors	Allows Most Innovation
Sidechains/ Layers/CUSF	Accumulates Trust	Actively Promotes Error- Correction	Allows Even Hardfork Style Innovation

Soft Forks Over Time

Part 3 of 4

Soft Forks Over Time

(according
to BitMex)

	Count of Ty		Colu ↗		
	Row Lal ↗	Quarters	Hard	Soft	UASF
Satoshi Era	⊖ 2009	Qtr1			Bitcoin Created!
		Qtr2			
		Qtr3			
		Qtr4			
	⊖ 2010	Qtr1			
		Qtr2			
		Qtr3	1	7	Ban many OP codes, but add the OP NOPs, and the Blocksize/SIGOPs limits.
		Qtr4			Dec 13, 2010 -- Last public activity from Satoshi.
Gavin Era	⊖ 2011	Qtr1			
		Qtr2			
		Qtr3			
		Qtr4			
	⊖ 2012	Qtr1		1	Ban identical TxIDs.
		Qtr2		1	Enable P2SH.
		Qtr3			
		Qtr4			
	⊖ 2013	Qtr1		2	Temp patch for BDB-lock divergence. + Require coinbase to include blockheight.
		Qtr2			
		Qtr3	1		Increase BDB lock limit.
		Qtr4			
	⊖ 2014	Qtr1			
		Qtr2			
		Qtr3			
		Qtr4			
"Scaling Bitcoin" Era	⊖ 2015	Qtr1			
		Qtr2			Gavin's last Github merge.
		Qtr3		1	DER sigs required.
		Qtr4		1	Add CLTV.
	⊖ 2016	Qtr1			
		Qtr2			
UASF Era		Qtr3		3	Add rLT, CLTV, and enforce median-time-past.
		Qtr4			3rd SB Conference, SegWit blockade begins.
	⊖ 2017	Qtr1			
		Qtr2			
		Qtr3			1
LN Era / Fork Era (?)		Qtr4			SegWit Activated.
					SegWit2x Fork Abandoned, Rise of BCH.
	⊖ 2018	Qtr1			
		Qtr2			
		Qtr3			
		Qtr4			LN capacity approaches 500 BTC for the first time.
	⊖ 2019	Qtr1			Present Day
		Qtr2			
		Qtr3			
		Qtr4			

Bitcoin's Ossification

original source code & edit history are mostly lost

Year	2009	2010	2011	2012	2013	2014	2015	2016
# of Soft Forks	0*	7	0	2	2	0	2	3

16

Year	2017	2018	2019	2020	2021	2022	2023	2024
# of Soft Forks	1	0	0	0	1	0	0	0 (Presumably)

2

- SegWit

- Announced Dec 2015
 - Coded Oct 2016
 - Activated Aug 2017
- } 20 Months

- Taproot

- Announced Jan 2018
 - Coded Oct 2020
 - Activated Nov 2021
- } 46 Months

Problems

- First – is it a problem ?
 - Some people don't want Bitcoin to “change” ...
 - ...but soft forks aren't a mandatory change. (The old software works.)
- Soft forks benefits:
 - Grant new options to users.
 - Improves the software; improve the money.
 - Multisig + Lightning (SegWit) were created via soft fork.
 - Security, (op vault), privacy, scalability require new soft forks.
- Soft forks costs...
 - Soft fork is basically free: SFs are optional, reversible, and inevitable.
 - **Optional** = The old protocol survives, so the upgrade is consensual.
 - **Reversible** = A soft fork claiming OP NOP 6 , for example, could be later deactivated by a 2nd soft fork, that just bans OP NOP 6.
 - **Inevitable** = If 51% hashrate mines a new version, then the soft fork activates – end of story.
 - Users who “resist” the soft fork, will break the heaviest-valid-chain rule and will hard fork.
 - Any soft fork that increases miner profitability, can and will activate, eventually.
- Cynical take: some prefer software NOT to improve, since they are middlemen.

CUSF

Core Untouched Soft Fork

“Ordinal-ization” of Soft Forks

“Sidechain-ziation” of Soft Forks

Part 4 of 4

CUSF - “Core Untouched Soft Fork”
*or: “Soft Forks, without a Soft Fork”,
or “The Ordinal-ization of Soft Forks”*

Paul Sztorc
v0.4.1 -- 6/23/2024

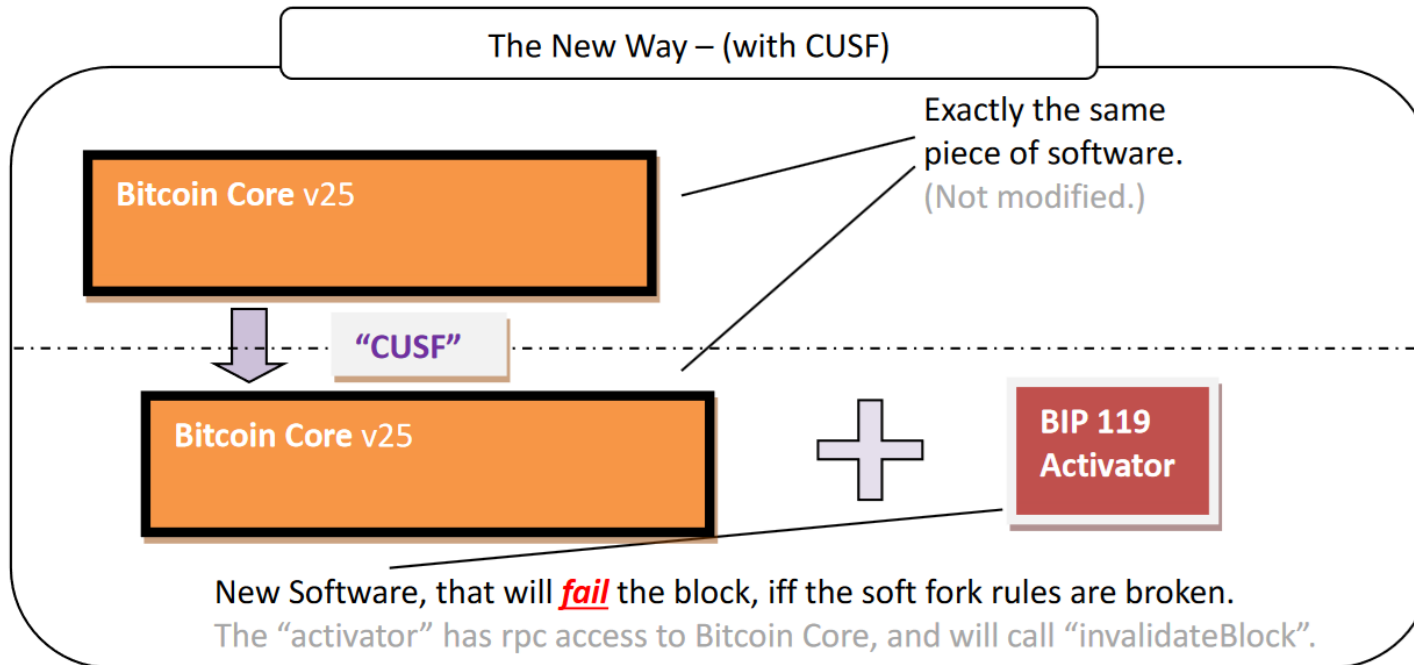
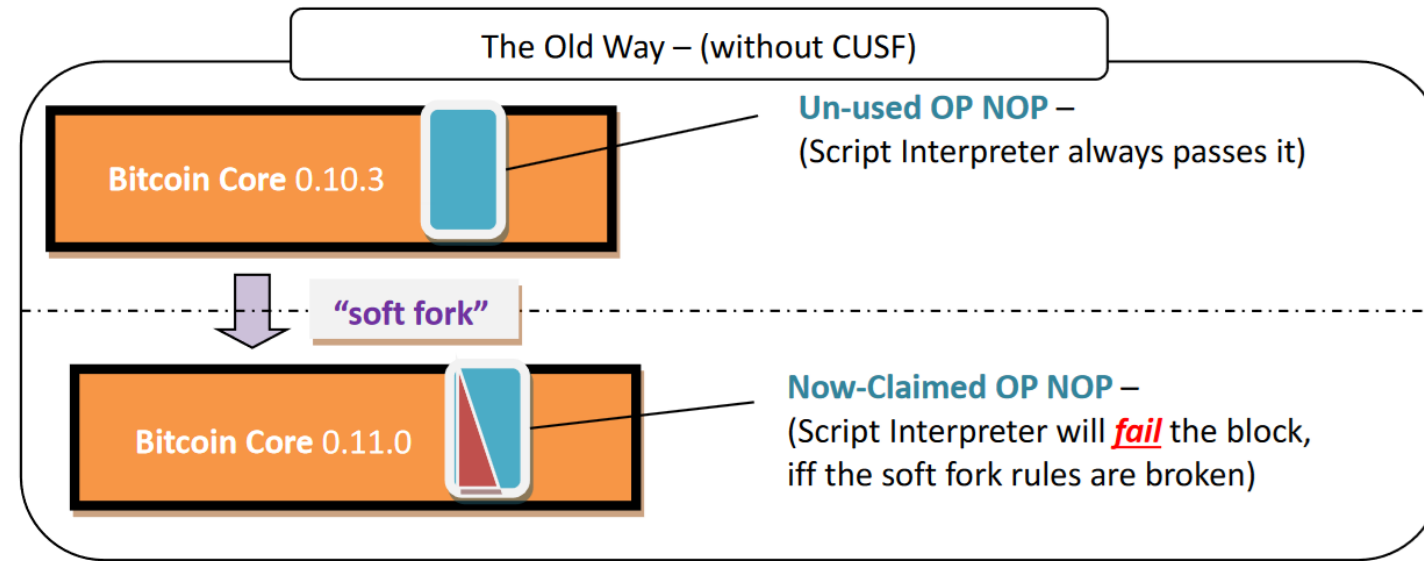
Summary

Each new soft fork (SF) should be a separate, standalone piece of software, “piloting” Bitcoin Core via the “invalidateblock” rpc. This makes soft forks faster, safer, and easier to understand -- ushering in a new age of Bitcoin Development.


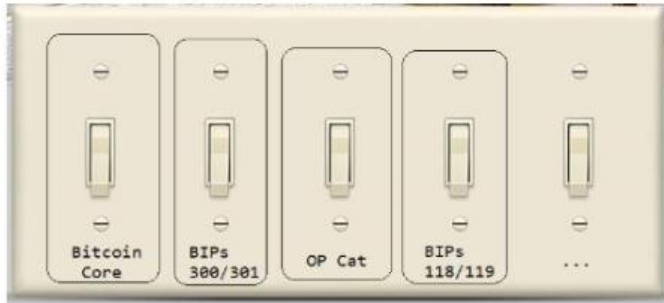
The Idea

The current soft fork process is so vague that arguably no one knows what it is -- but it certainly involves opening a GitHub pull request. Here, I present an alternative process: put new soft fork validation rules in their own, separate piece(s) of software. This software can use “getblock” and “invalidateblock” (via rpc access to Bitcoin Core) to enforce new consensus rules. This has many advantages.

- Paper at: <https://bip300cusf.com>
- Soft fork via a 2nd piece of software –
 - Takes blocks from Bitcoin Core, and gives them a “second pass”.
 - Calls `invalidateblock` in Bitcoin Core if new rulebreaking.



- Same effect
- But two software daemons
- Two RPC servers
- “Inefficient” for computer – 2x as much work
- But “separable” at the human level – socially scalable.
- Simple change, many advantages

	Before CUSF	After CUSF
How are SFs perceived by the layperson?	 <p>SFs are <u>surgery</u>, on our beloved only child.</p> <p>One software (Bitcoin Core) that is “changed” in a permanent, and poorly-understood way.</p>	 <p>SFs are just other apps “on top” of Bitcoin L1 – similar to ordinals.</p> <p>We turn these apps on/off, the same way we’d turn anything else on/off. They are modular and safe.</p>

	<u>Before CUSF</u>	<u>After CUSF</u>
How are SFs activated?	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Think of the idea. 2. Discuss on bitcoin-dev (mailing list). 3. Write code for testnet/regtest version. 4. Test on Inquisition / similar. 5. ??? Get feedback from users / Twitter 6. Spend 20+ hours rebasing your SF to the latest version of Bitcoin Core. 7. Open pull request. 8. Reply to PR-Feedback on GitHub. 9. Repeat steps 5-8, every 3 months for 2 years. 10. Pull request is merged. (?) (Or not.) 11. Activation logic is merged. 12. Debates about activation, Bip9/8, Speedy Trial, LoT=true, Hashrate Thresholds, UASF -- virtue signaling on Twitter -- 13. Speedy Trial (or whatever), is yolo'ed by someone. 14. Months later, 90% hashrate finally upgrades -- even though they don't really understand what the SF is or what it does. 15. People start using the feature. 	<p>Follow these steps:</p> <ol style="list-style-type: none"> 1. Think of an idea. 2. Write the code. 3. Write a document, explaining how your idea boosts miner profits. (Either via a higher BTC price, or via more txn fees.) 4. Miners (ie Pools) run your software, alongside their existing software. (They can stop running it at any time.) 5. Users also run your software, and start using the feature.

	<u>Before CUSF</u>	<u>After CUSF</u>
How do you de-activate the fork?	This is so difficult, that it has never happened. It involves: * A hard fork (ie, a disaster), OR * A new soft fork, that censors the 1 st SF at the txn level (ie, bikeshedding & authority).	Very easy – people stop running the Activator software. The SF just naturally de-activates.
Speed / ease of Innovation?	SFs are always SLOW and academic. “Like replacing an aircraft engine, while the plane is in the air”.	SFs can be FAST and experimental – they can be like startups. They can fail without bothering anyone.
How is each SF <u>justified</u> to the layperson?	We need <u>to explain to people</u> why the SF is safe.	It is <u>obvious</u> that SFs are safe. No existing users can even <u>detect</u> a CUSF. SFs are pushed to the mining side where they belong.
Who must agree to run the SF?	Users of the New Feature, + + 51% Hashrate, + All BCMs, + All who rely on Bitcoin Core	Users of the New Feature, + + 51% Hashrate
What is the Guiding Principle of the Yes/No Activation Decision?	Does this SF “have consensus”? (This is an unfalsifiable theory in practice – it also defeats the original purpose of the hard/SF distinction. At best, it is very hard to measure – at worst it is an unfalsifiable theory.) Will the code be easy to merge/maintain/run ?	Will running this software <u>increase miner profits</u> ?

	<u>Before CUSF</u>	<u>After CUSF</u>
Who can be negatively affected by a fork? (In a way other than a reorg.)	BCMs: they must... ...evaluate the SF-code. ...maintain the SF-code in perpetuity (if merged). ...release an emergency fix if something goes wrong.	Only those who <u>choose</u> to opt-in to the new feature. (Note: this includes 51% hashrate, since –in order to have reached this point— they must have opted-in.)
What are today's Developer Incentives?	Bad – we must trust today's BCMs. (Trust them to only make the “right” changes.) Low oversight (or even understanding). BCMs are hard to fire or replace. Each change makes the software code harder for a newbie to learn.	Good – anyone can become a Bitcoin developer at any time. Or leave. Devs compete <u>against</u> each other – (competition keeps developers honest). Developers are accountable to <u>a neutral external metric</u> (mining profits), not a corrupt USSR-style bureaucracy “popularity contest”.
Effect on “job security” of BCMs?	Enormous “job security” for BCMs.	Job security decreases. SF innovators can do whatever they like, without needing permission from BCMs. BCM role fades into irrelevance as they become more replaceable “maintenance” workers.
What form can the new code take?	The SF must be in C++. It must be a GitHub/Bitcoin pull request. It must obey the style guides & naming conventions & code architecture of GitHub/Bitcoin.	The SF can take any form. It can be written in any programming language. It can use any style/naming convention.

	<u>Before CUSF</u>	<u>After CUSF</u>
How might we port the SF to an Altcoin?	The SF would have to be rewritten. A new set of _CMs will be inconvenienced.	Can be freely reused by <u>any</u> L1. (So, Litecoin, Monero, whatever, they can have their own BIP 119/118, without changing their own code.)
How important is code review?	Review is essential.	Review is unnecessary.
Can anyone obstruct the process, and get away with it (without accountability)?	Core devs have a veto (incl. silent veto & pocket veto) , can demand changes in style, formate, language, readability – these can be time-wasting filibuster changes.	Core devs do not necessarily need to be consulted. (Note: miners may <u>voluntarily consult</u> 3 rd party expert advisors, and <u>choose</u> to follow their advice.)
Toxic Incentives	The high 90% Activation Threshold results in “toxic limbo”: where 2 (or more) 11%-hashrate-coalitions can emerge, and make mutually inconsistent demands – resulting in minority gridlock.	The 50% hashrate threshold is simple, logical, and internally consistent. No 3 rd parties have a veto.

Download Today – OP CAT & BIP300

Enforcers

Enforcers are standalone software meant to be used by people operating full nodes, to verify that their nodes are in compliance with the new soft fork rules to be implemented.

OP CAT 🐱

Download OP CAT Enforcer

Auditor

BIP300 🚗 🧑🏻

Download BIP300 Enforcer

Sidechain

Blockmaker

The blockmaker hacks getblocktemplate, to set a priority fee of -21M btc, for every txn rejected by any Enforcer. Therefore, miners who run this, will never have their blocks rejected by any Enforcer.

Download Blockmaker

bip300cusf.com/download

(This is one easy way of solving all of our soft fork problems.)

The End

- Paul Sztorc
 - layertwolabs.com ;
 - truthcoin.info
 - bitcoinhivemind.com
 - drivechain.info
- Twitter: @truthcoin ; Telegram: @psztorc

Please Ask Your
Questions Now

New Soft Forks ??

- Is there even still a process?
- SegWit Trauma / PTSD
 - Unsolved mysteries of the Blocksize war
 - Why did people get hashrate support for a hard fork, when hashrate is irrelevant to a hard fork? I don't know.
 - Miners signed a meaningless piece of paper backing the wrong side, but they never actually did anything. Yet still they feel guilty and unwilling to do further soft forks.
- Ratio of Experts / Laypeople is plummeting. More Ls, harder to E.
- Sour Grapes

New Soft Forks ??

- Is there even still a process?
- SegWit Trauma / PTSD
 - Unsolved mysteries of the Blocksize war
 - Why did people get hashrate support for a hard fork, when hashrate is irrelevant to a hard fork? I don't know.
 - Miners signed a meaningless piece of paper backing the wrong side, but they never actually did anything. Yet still they feel guilty and unwilling to do further soft forks.
- Ratio of Experts / Laypeople is plummeting. More Ls, harder to E.
- Sour Grapes
- The real reason....

 gavin
Create


<> Code

Embed

The Real Reason...

Revisions

Split Unified

 gavinandresen revised this gist on Jun 29, 2012.

1 changed file with 4 additions and 0 deletions.

4 BitcoinVersioning.md

@@ -2,6 +2,10 @@

2 2

3 3

We recently rolled out two changes to the Bitcoin block acceptance rules (BIP16 and BIP30); this document records the lessons learned and makes recommendations for handling future blockchain rule changes.

4 4

+ Note: there are "soft" rule changes and "hard" rule changes. "Soft" changes tighten up the rules-- old software will accept all the blocks and transactions created by new software, but the opposite may not be true. "Soft" changes do not require the entire network of miners and merchants and users to upgrade or be left behind.

6 +

7 +

"Hard" changes modify the rules in a way that old, un-upgraded software consider illegal. At this point it is much, much more difficult (some might say impossible) to roll out "hard" changes, because they require every miner and merchant and user to upgrade.

8 +

5 9

Lessons Learned

6 10

7 11

+ Be sure to consider all 4 combinations of old/new software running before/after the majority of the network supports the new rule(s).

Jameson Lopp's Article



Gwern's Article

