

Soft Forks, Governance, Culture

MIT Bitcoin Expo

April 22, 2023

Paul Sztorc

Agenda

1. Soft Forks

1. The Basics
2. Four Comments

2. Governance

1. A useful definition, in a P2P context
2. The Big Three
3. The Governance Table

3. Culture

1. Soft Forks Over Time
2. Conventional Wisdom, vs Fundamental Analysis
3. A Simple explanation that ties it all together

Soft Forks

Part 1 of 3

Soft Forks – The Basics

- Soft vs Hard
 - “Tighten Rules” vs “Loosen Rules”
 - Optional 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)

Soft Forks – Some Useful History

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

 [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
4 4 lessons learned and makes recommendations for handling future blockchain rule changes.
5 + Note: there are "soft" rule changes and "hard" rule changes. "Soft" changes tighten up the rules-- old software will accept
6 + all the blocks and transactions created by new software, but the opposite may not be true. "Soft" changes do not require
7 + the entire network of miners and merchants and users to upgrade or be left behind.
8 +
9 + "Hard" changes modify the rules in a way that old, un-upgraded software consider illegal. At this point it is much, much
10 + more difficult (some might say impossible) to roll out "hard" changes, because they require every miner and merchant and
11 + user to upgrade.
12 +
13 ## Lessons Learned
14
15 + Be sure to consider all 4 combinations of old/new software running before/after the majority of the network supports the
16 + new rule(s).
```

Forbidden, on grounds of impracticality

In Blockchain, Fork Has a Strange Meaning

Culinary Fork?



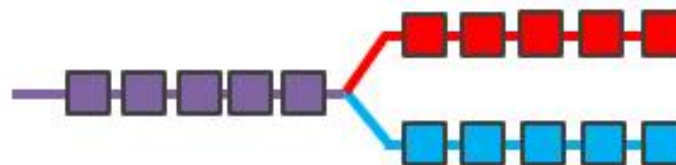
Tuning Fork?



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

- 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!

Governance

Part 2 of 3

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 with hyphens: "gov·er·nance". To the right of this is a pronunciation guide: "'gə-vər-nən(t)s" with a speaker icon. Below the pronunciation guide is the plural form "plural **governances**".

Below the plural form is a link for "Synonyms of governance >".

The definition is provided 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'. A search bar contains the word 'governance' with a magnifying glass icon. On the left side, there is a sidebar with the Merriam-Webster logo (Est. 1828) and a 'Dictionary' label. Below this, a red banner highlights the 'Definition' section. Other sidebar options include 'Synonyms', 'Example Sentences', 'Word History', and 'Phrases Containing'. The main content area displays the word 'governance' as a noun, followed by 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

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**

- Rejects P2P

Governance – Definition



The screenshot shows the Merriam-Webster website with the word 'governance' searched. The left sidebar contains navigation links: Dictionary, Thesaurus, Games & Quizzes, Thesaurus, Features, and Word Finder. 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

- ▲ 2 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?
- ▼ 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"

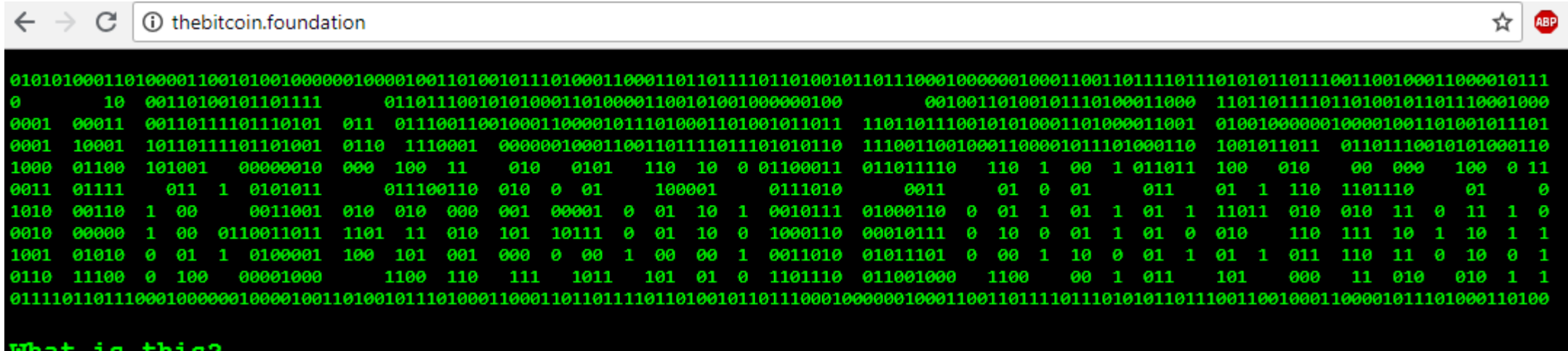
1. Soft fork means that different pieces of software can coexist
2. Anything in the "Line of Coexistence" is fair game!

"Latest
Core"

"Static"
Protocol

"Linear
Coexistence"
(Consent-
Based)

The “Static Protocol” Position



```
0101010001101000011001010010000001000010011010010111010001100011011011101101001011011100010000001000110011011110111010101101110011001000010111
0      10  00110100101101111      01101110010101000110100001100101001000000100      00100110100101110100011000      11011011110110100101101110001000
0001 00011 00110111101110101 011 0111001100100011000010111010001101001011011 1101101110010101000110100011001 01001000000100001001101001011101
0001 10001 10110111101101001 0110 1110001 000000100011001110111011101010110 11100110010001100001011101000110 1001011011 01101110010101000110
1000 01100 101001 00000010 000 100 11 010 0101 110 10 0 01100011 011011110 110 1 00 1 011011 100 010 00 000 100 0 11
0011 01111 011 1 0101011 011100110 010 0 01 100001 0111010 0011 01 0 01 011 01 1 110 110110 01 0
1010 00110 1 00 0011001 010 010 000 001 00001 0 01 10 1 0010111 01000110 0 01 1 01 1 01 1 11011 010 010 11 0 11 1 0
0010 00000 1 00 0110011011 1101 11 010 101 10111 0 01 10 0 1000110 00010111 0 10 0 01 1 01 0 010 110 111 10 1 10 1 1
1001 01010 0 01 1 0100001 100 101 001 000 0 00 1 00 00 1 0011010 01011101 0 00 1 10 0 01 1 01 1 011 110 11 0 10 0 1
0110 11100 0 100 00001000 1100 110 111 1011 101 01 0 1101110 011001000 1100 00 1 011 101 000 11 010 010 1 1
0111101101110001000000100001001101001011101000110001101101111011010010110111000100000010001100110111101101011011100110010001100001011101000110100
```

What is this?

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!

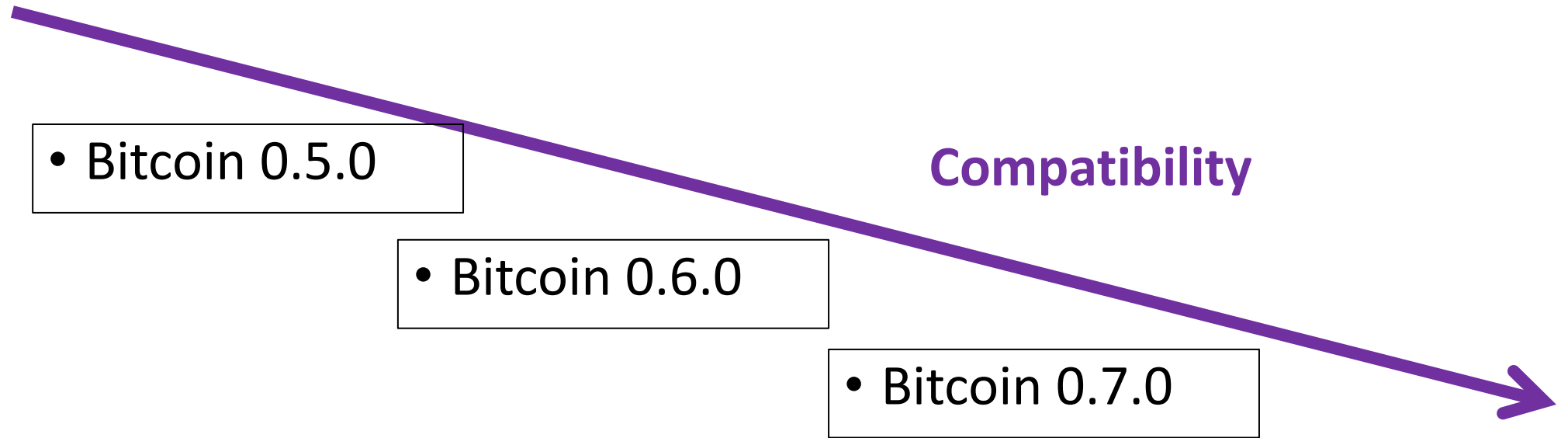
"Latest
Core"

"Static"
Protocol

"Linear
Coexistence"
(Consent-
Based)

Upgrading via Soft Fork

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



Governance Strategies... And their Problems

| | Problem of Expertise | The Euthyphro Dilemma / Fallibilism | Problem of Innovation / “Dissent” | Social Attack / Charisma (Constant Vigilance Needed) |
|--------------------------------------|----------------------|-------------------------------------|-----------------------------------|--|
| “Latest Core” | | | | |
| “Static” Protocol | | | | |
| “Linear Coexistence” (Consent-Based) | | | | |
| | | | | |

The Euthyphro Dilemma

Bitcoin.org can tell us that some software is "Bitcoin"

God tell us something is good...

God is a professor /
advisor
who knows more
about morality than us

God's opinion is the only
opinion

Divine Command Theory

We could have learned
morality without His help.
He merely sped us up.

We can't learn morality
without God's
instructions... But...

...God can
change his
mind.

...we can later learn that we misunderstood God.

The Euthyphro Dilemma

Bitcoin.org can tell us that some software is "Bitcoin"

God tell us something is good...

God is a professor /
advisor
who knows more
about morality than us

God's opinion is the only
opinion

Divine Command Theory

Fallibilism

We could have learned
morality without His help.
He merely sped us up.

We can't learn morality
without God's
instructions... But...

...God can
change his
mind.

...we can later learn that we misunderstood God.

Governance Strategies... And their Problems

| | Problem of Expertise / Charisma Attack | The Euthyphro Dilemma / 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 | The Euthyphro Dilemma / 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 | |
| | | | |

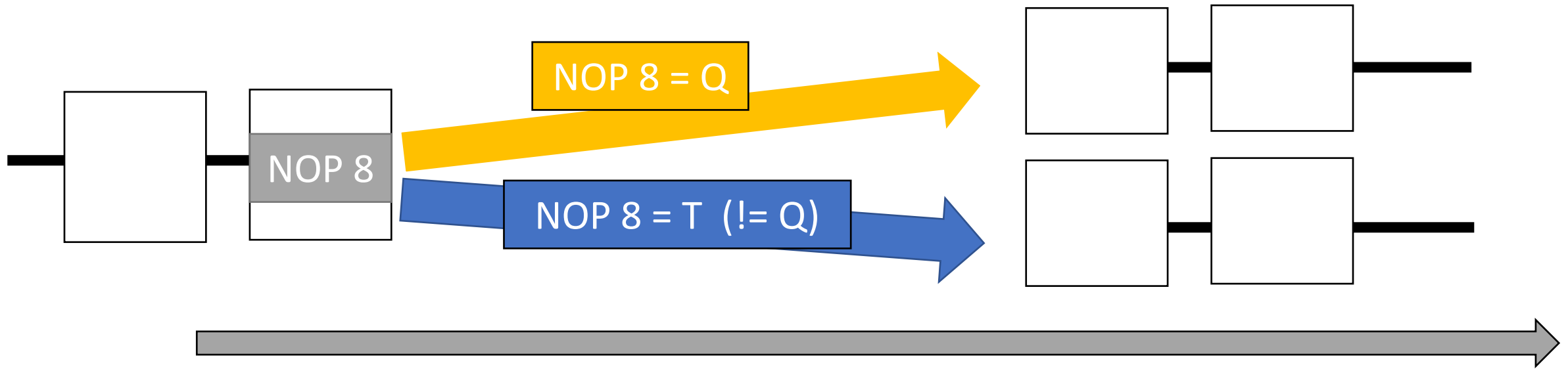
Expertise... is Mandatory!

- 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

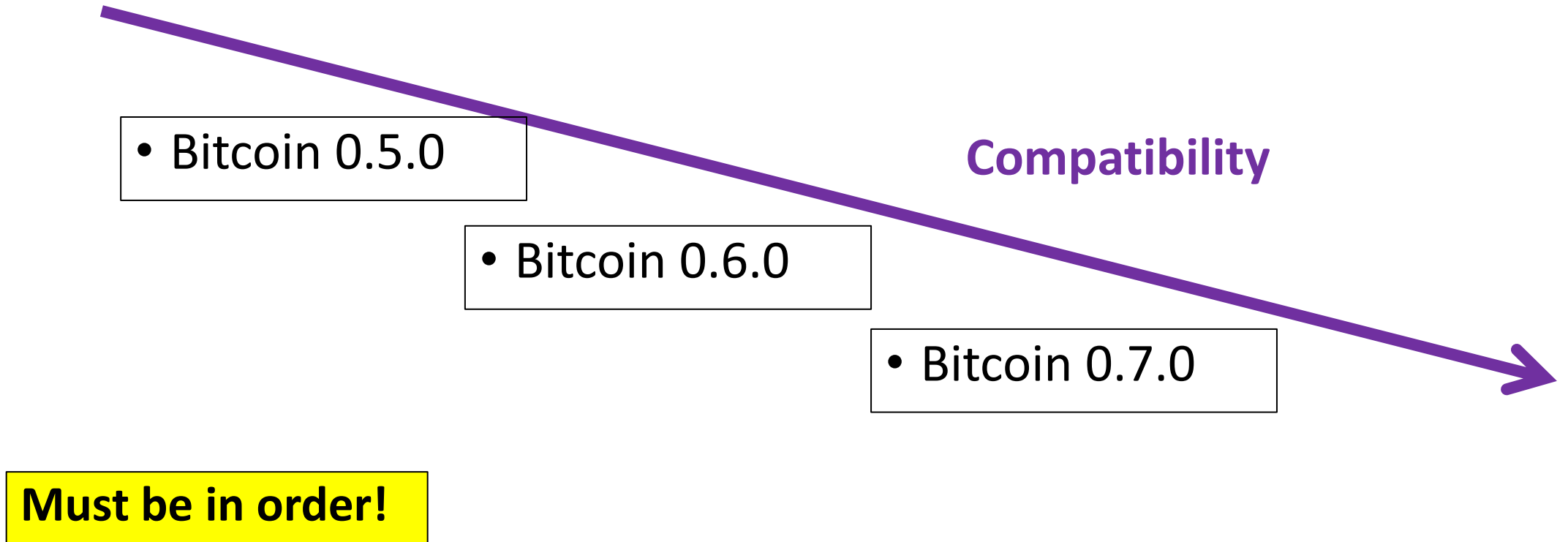
| | Problem of Expertise / Charisma Attack | The Euthyphro Dilemma / Fallibilism | Problem of Innovation / “Dissent” |
|--------------------------------------|--|--|-----------------------------------|
| “Latest Core” | No Laypeople Allowed | Outsource Your Thinking to Bitcoin.org | |
| “Static” Protocol | 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

...just about everything!



Governance Strategies... And their Problems

| | Problem of Expertise / Charisma Attack | The Euthyphro Dilemma / 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 | The Euthyphro Dilemma / 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 | The Euthyphro Dilemma / 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 |
| The Sidechain Vision | Accumulates Trust | Actively Promotes Error- Correction | Allows Even Hardfork Style Innovation |

Culture

Part 3 of 3

Soft Forks Over Time

(according
to BitMex)

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

Bitcoin's Ossification

| | | | | | | | | | |
|---|-----------------|------|------|------|------|------|------|-------------------|----|
| • | Year | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 16 |
| | # of Soft Forks | 7 | 0 | 2 | 2 | 0 | 2 | 3 | |
| | Year | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2 |
| | # of Soft Forks | 1 | 0 | 0 | 0 | 1 | 0 | 0 (Presumably) | |

- SegWit

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

- Taproot

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

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

<> [icon] ...

@@ -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).

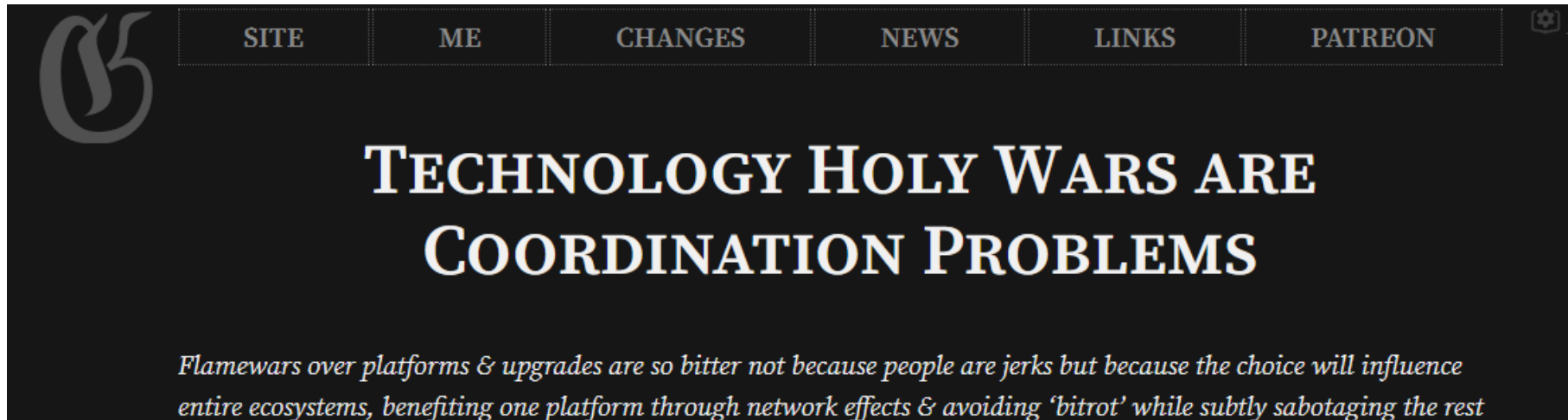
Jameson Lopp's Article


MAR 25, 2023 • 41 MIN READ • BITCOIN

A History of Bitcoin Maximalism

Bitcoin Maximalism isn't what most people think it is, but there is a logical explanation for how it transformed into what we see today.

Gwern's Article

The image shows the header of Gwern's article. It features a dark background with a navigation bar at the top containing links for SITE, ME, CHANGES, NEWS, LINKS, and PATREON. A large, stylized 'G' logo is on the left. The main title is in a large, white, serif font, and the subtitle is in a smaller, italicized, white, serif font.

 [SITE](#) [ME](#) [CHANGES](#) [NEWS](#) [LINKS](#) [PATREON](#)

TECHNOLOGY HOLY WARS ARE COORDINATION PROBLEMS

Flamewars over platforms & upgrades are so bitter not because people are jerks but because the choice will influence entire ecosystems, benefiting one platform through network effects & avoiding 'bitrot' while subtly sabotaging the rest

The End

About Me

- Paul Sztorc, Founder and CEO, LayerTwo Labs –
“Making every transaction on Earth, a Bitcoin Txn”
- Sites: layertwolabs.com ; truthcoin.info ; bitcoinhivemind.com ; drivechain.info
- Many essays, “Nothing is Cheaper Than Proof of Work”, “Measuring Decentralization”
- Author of BIPs 300 and 301.
- Twitter: @truthcoin ; Telegram: @psztorc

Questions?