CUSF

1) Scale Bitcoin to 8 billion people
2) No changes to Bitcoin Core
3) Collect Billions in Txn Fees

OP NEXT
Nov 9, 2024
Boston MA
Paul Sztorc

Agenda

1. Background, Context – 15 mins
2. CUSF (the solution) – 5 mins
3. Q & A – 10 mins

My History

- Scaling I, II, III (Sept 2015) → This conference (?)
- “Truthcoin” (Dec 2013) → BitcoinHivemind.com → [other ppl] PolyMarket
- “Measuring Decentralization” (Sept 2015) → “Drivechain” (Nov 2015) → BIP-300
- “Sidechain Privatization” (Jun 2016) → Blind Merged Mining (Jan 2017) → BIP-301 → proposer-builder separation
- “Win-Win Blocksize Solution” (July 2015) → “Fork Futures”
- BitAssets (Jun 2018) → [other ppl] Ordinals , Coordinate , ERC20
- “Better Fork Terminology” (Dec 2016) → MIT talk (2023) → CUSF (2024)

Fee Comparison

This diagram *is to scale*.

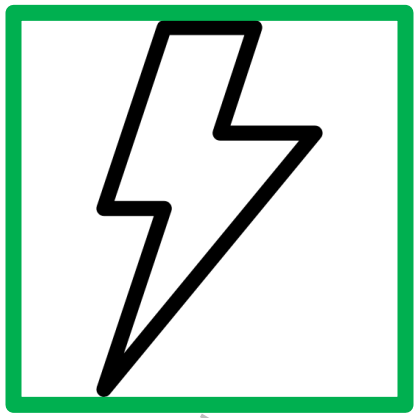
$128 million
(fee revenue 2022)

$767 million
(fee revenue 2023 – the ordinals year)

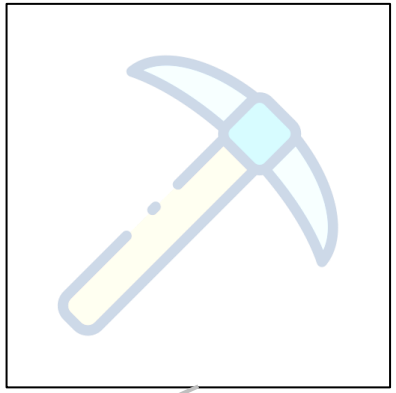
$3.0 billion
(All-Altcoin Fee Revenue 2022)

$640 billion
(Earth’s 6.4 trillion txn X $0.10 , 2022)

Non-Mined L2s
vs
Mined L2s



Non-Mined L2s



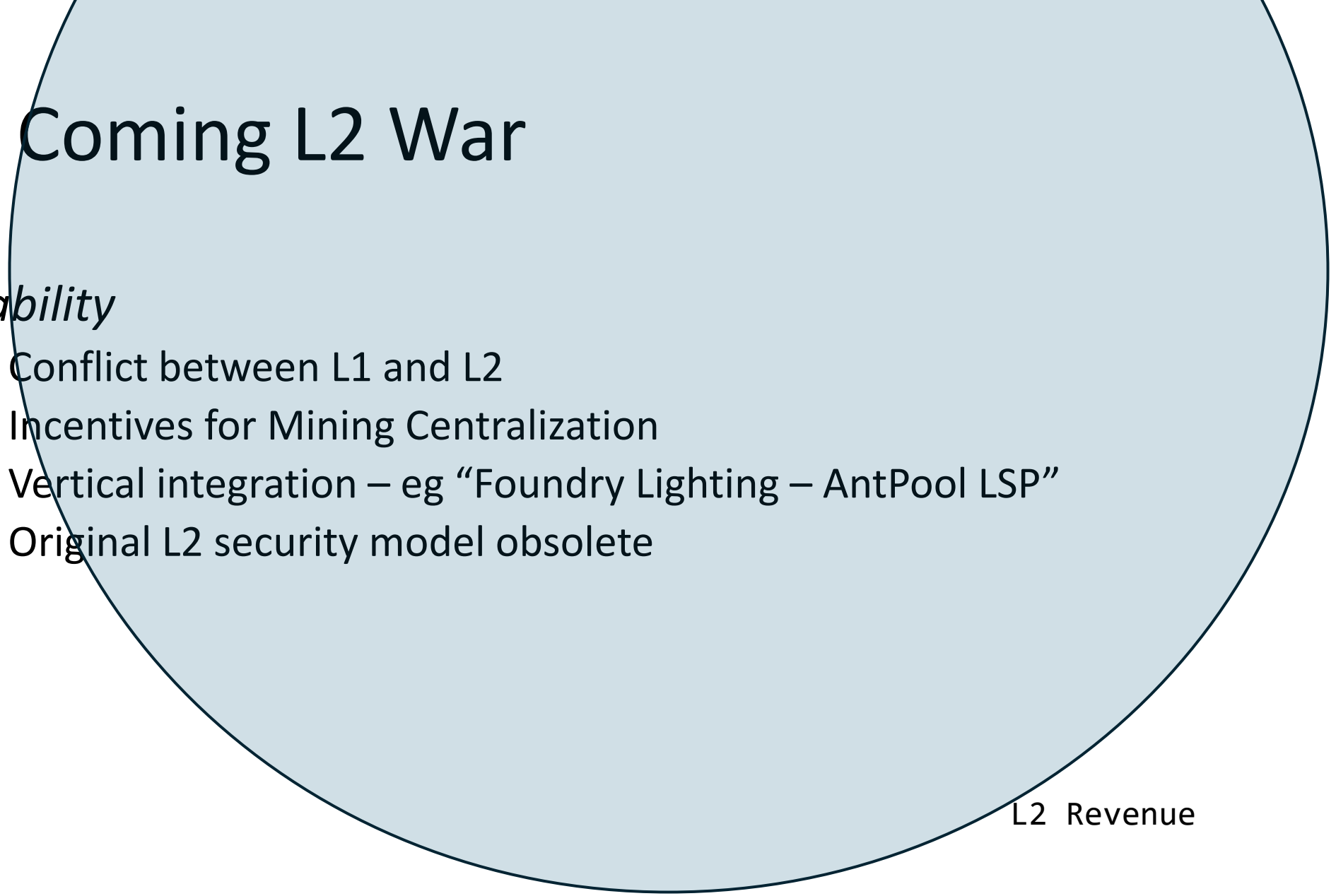
Mined L2s

L1

$640 billion

The Coming L2 War

- *Instability*
  1. Conflict between L1 and L2
  2. Incentives for Mining Centralization
  3. Vertical integration – eg “Foundry Lighting – AntPool LSP”
  4. Original L2 security model obsolete



Every L2 is vulnerable to 51% attack by miners

[Lightning-dev] New form of 51% attack via lightning's revocation system possible?

René Pickhardt r.pickhardt at googlemail.com
Tue Mar 13 13:30:21 UTC 2018

Since according to the spec channels should never be balanced worse than 99% to 1% the attacker could steal up to 99% of all the bitcoins allocated in the sum of all payment channels the attacker was connected to. This amount could obviously be way higher than just double spending her own funds. This attack would be interesting in particular for the power nodes created by the Barabasi-Albert model of lnd's autopilot (c.f.: https://github.com/lightningnetwork/lnd/issues/677).

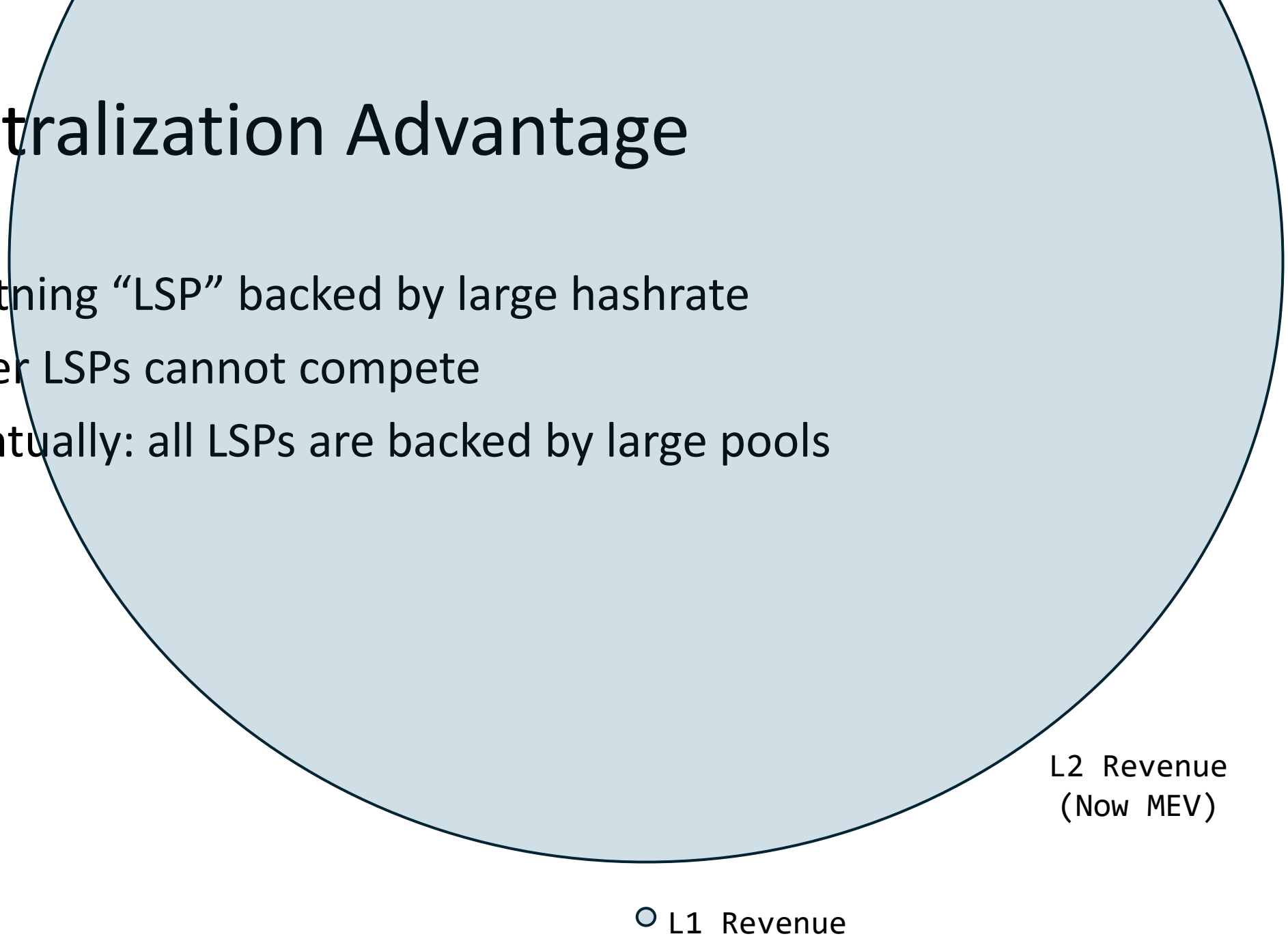
I understand that with the growth of the bitcoin (mining) network a 51% attack becomes less and less likely. Also I am very happy to be proven false about the attack that I am describing.

Another sad thing about this attack is that I currently do not see any (reasonable) way of preventing this form of a 51% attack (other than creating payment channels that don't offer the possibility of revocation) as it is abusing exactly the core idea of lightning to do something in

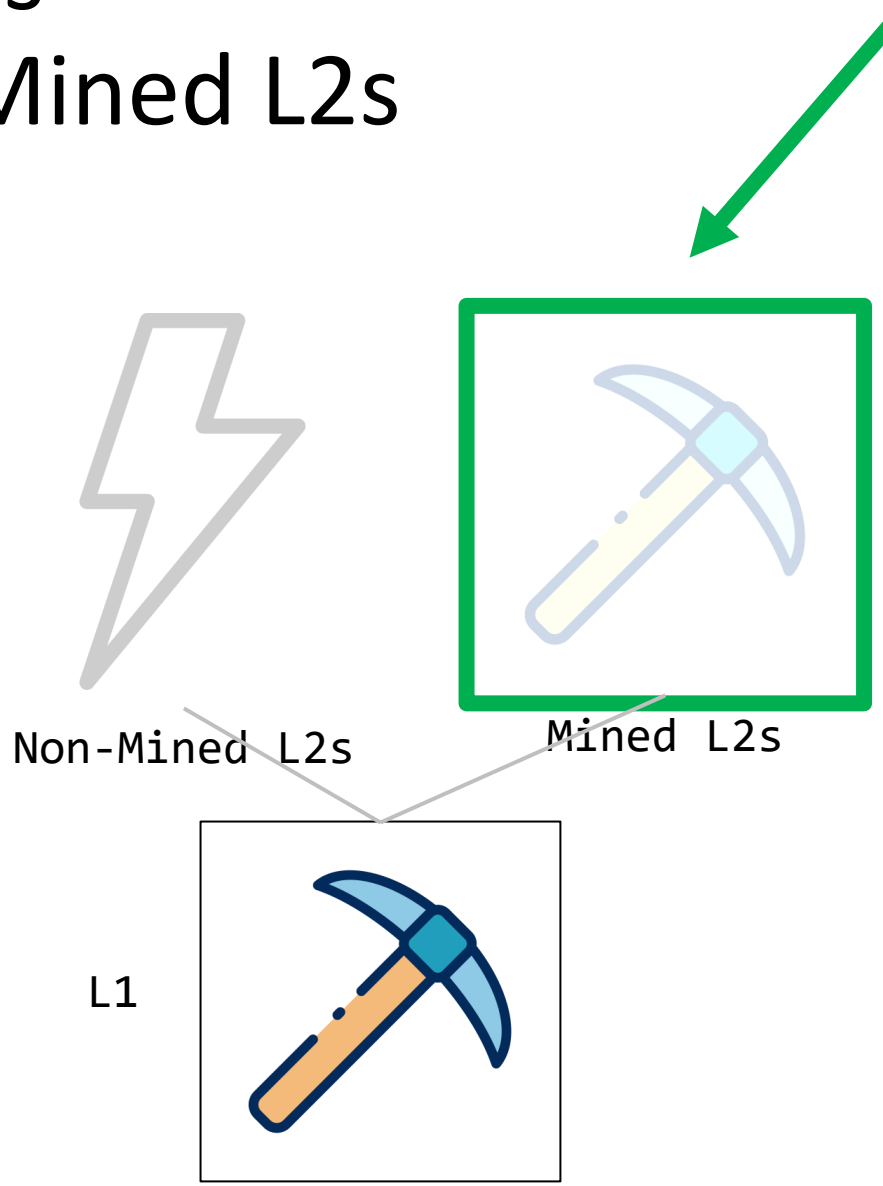
onboard, offboard, and “justice” txns on L1 can all be censored

Centralization Advantage

- Lightning “LSP” backed by large hashrate
- Other LSPs cannot compete
- Eventually: all LSPs are backed by large pools



Non-Mined L2s
vs
Mined L2s



$640 billion

My Proposal 13-13

Sidechains for Scaling -- Thunder Network

05 Feb 2021

Smallblock Chain

1 1

Throughput: 1
O(n^2) Cost: 1

Largeblock Chain (No Sidechains)

8 64

Throughput: 8
O(n^2) Cost: 64

Lightning Network

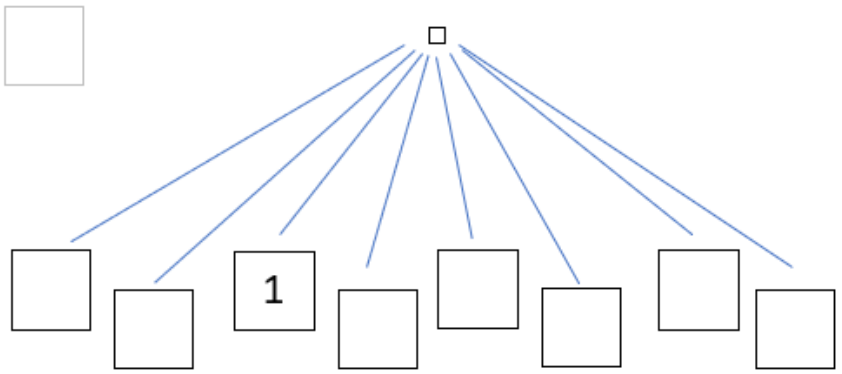
1 1

ε

Many ε (other people's L
txns) that you disregard

Throughput: 8
O(n^2) Cost: 1+ε

Thunder Network



A total of 8 sidechains (each 1MB), 7 of which you disregard.

Throughput: 8
O(n^2) Cost: 1+ε

All the World's Txns

03 May 2024

Txn Growth Rate				# of L2 chains	Blocks Per Year	Bytes per Txn	
	6.20%			13	52596	138	
Year	World Txns/Year	BTC Adoption (% of world txns)	On-chain Txns/Year	Txns per chain	Txns per block	Imputed Blocksize Limit (megabytes per 10min)	6 Month Chain-History Size (terabytes)
2024	6.40E+12	1.00%	6.40E+10	4.92E+09	9.36E+04	12.92	0.340
2025	6.80E+12	2.00%	1.36E+11	1.05E+10	1.99E+05	27.44	0.722
2026	7.22E+12	5.00%	3.61E+11	2.78E+10	5.28E+05	72.84	1.916
2027	7.67E+12	10.00%	7.67E+11	5.90E+10	1.12E+06	154.72	4.069
2028	8.14E+12	20.00%	1.63E+12	1.25E+11	2.38E+06	328.62	8.642
2029	8.65E+12	50.00%	4.32E+12	3.33E+11	6.32E+06	872.48	22.944
2030	9.18E+12	100.00%	9.18E+12	7.06E+11	1.34E+07	1853.15	48.734
2031	9.75E+12	100.00%	9.75E+12	7.50E+11	1.43E+07	1968.04	51.756
2032	1.04E+13	100.00%	1.04E+13	7.97E+11	1.51E+07	2090.06	54.964
2033	1.10E+13	100.00%	1.10E+13	8.46E+11	1.61E+07	2219.65	58.372
2034	1.17E+13	100.00%	1.17E+13	8.98E+11	1.71E+07	2357.26	61.991

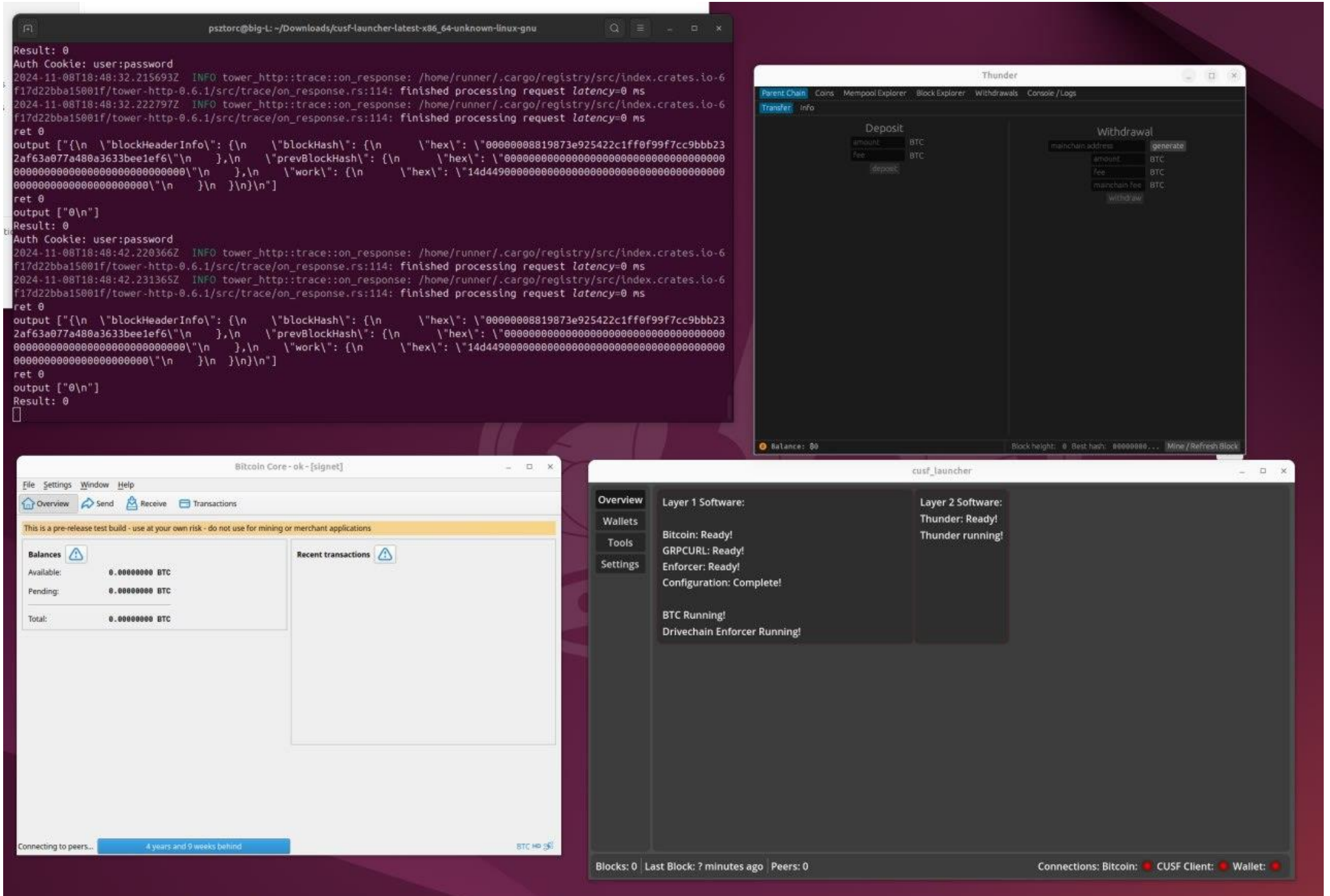
	Lightning	Custodial	Thunder
Each Onboard Needs Layer-1 Bytes	**Yes** (made up of channels, channels have an owner defined on Layer1)	**No** (made of UTXOs, UTXO owner is defined on layer2, transferrable)	**No** (made of UTXOs, UTXO owner is defined on layer2, transferrable)
Periodic Layer-1 Txns Needed	Yes	No	No
Payment Capacity	Limited to *lowest* capacity along the route.	Unlimited	Unlimited
Payment Reliability ("Routing")	Only as reliable as the *least* reliable member along the route.	High	High
Cost if Payment Fails	Funds locked for Days	Payments Don't Fail	Payments Don't Fail
Payment Speed	Instant	Instant	Cor Update: Instant** ed
Receive Money While Offline	No	Yes	Yes
Minimum Payment Value	Roughly (1/3) of the *Layer1* fee.*	No	No
Custodial	No	Yes	No
Relationship to L1 Miner Revenues* **	Directly Adversarial	Directly Adversarial	Perfectly Aligned

	Lightning	Custodial	Thunder
Each Onboard Needs Layer-1 Bytes	**Yes** (made up of channels, channels have an owner defined on Layer1)	**No** (made of UTXOs, UTXO owner is defined on layer2, transferrable)	**No** (made of UTXOs, UTXO owner is defined on layer2, transferrable)
Periodic Layer-1 Txns Needed	Yes	No	No
Payment Capacity	Limited to *lowest* capacity along the route.	Unlimited	Unlimited
Payment Reliability ("Routing")	Only as reliable as the *least* reliable member along the route.	High	High
Cost if Payment Fails	Funds locked for Days	Payments Don't Fail	Payments Don't Fail
Payment Speed	Instant	Instant	Cor Update: Instant** ed
Receive Money While Offline	No	Yes	Yes
Minimum Payment Value	Roughly (1/3) of the *Layer1* fee.*	No	No
Custodial	No	Yes	No
Relationship to L1 Miner Revenues* **	Directly Adversarial	Directly Adversarial	Perfectly Aligned

	Lightning	Custodial	Thunder
Each Onboard Needs Layer-1 Bytes	**Yes** (made up of channels, channels have an owner defined on Layer1)	**No** (made of UTXOs, UTXO owner is defined on layer2, transferrable)	**No** (made of UTXOs, UTXO owner is defined on layer2, transferrable)
Periodic Layer-1 Txns Needed	Yes	No	No
Payment Capacity	Limited to *lowest* capacity along the route.	Unlimited	Unlimited
Payment Reliability ("Routing")	Only as reliable as the *least* reliable member along the route.	High	
Cost if Payment Fails	Funds locked for Days	Payments Don't Fail	Payments Don't Fail
Payment Speed	Instant	Instant	Cor Update: Instant** ed
Receive Money While Offline	No	Yes	
Minimum Payment Value	Roughly (1/3) of the *Layer1* fee.*	No	
Custodial	No	Yes	No
Relationship to L1 Miner Revenues* **	Directly Adversarial	Directly Adversarial	Perfectly Aligned

+ Fast Cashouts from Pools to Hashers

+ Does not require changes to Bitcoin Core (but does require CUSF)


psztorc@big-L: ~/Downloads/cusf-launcher-latest-x86_64-unknown-linux-gnu
Result: 0
Auth Cookie: user:password
2024-11-08T18:48:32.215693Z INFO tower_http::trace::on_response: /home/runner/.cargo/registry/src/index.crates.io-6f17d22bba15001f/tower-http-0.6.1/src/trace/on_response.rs:114: finished processing request latency=0 ms
2024-11-08T18:48:32.222797Z INFO tower_http::trace::on_response: /home/runner/.cargo/registry/src/index.crates.io-6f17d22bba15001f/tower-http-0.6.1/src/trace/on_response.rs:114: finished processing request latency=0 ms
ret 0
output ["{\n \"blockHeaderInfo\": {\n \"blockHash\": {\n \"hex\": \"00000008819873e925422c1ff0f99f7cc9bbb232af63a077a480a3633bee1ef6\"\n },\n \"prevBlockHash\": {\n \"hex\": \"0000000000000000000000000000000000000000000000000000000000000000\"\n },\n \"work\": {\n \"hex\": \"14d4490000000000000000000000000000000000000000000000000000000000\"\n }\n }\n}\n"]
ret 0
output ["0\n"]
Result: 0
Auth Cookie: user:password
2024-11-08T18:48:42.220366Z INFO tower_http::trace::on_response: /home/runner/.cargo/registry/src/index.crates.io-6f17d22bba15001f/tower-http-0.6.1/src/trace/on_response.rs:114: finished processing request latency=0 ms
2024-11-08T18:48:42.231365Z INFO tower_http::trace::on_response: /home/runner/.cargo/registry/src/index.crates.io-6f17d22bba15001f/tower-http-0.6.1/src/trace/on_response.rs:114: finished processing request latency=0 ms
ret 0
output ["{\n \"blockHeaderInfo\": {\n \"blockHash\": {\n \"hex\": \"00000008819873e925422c1ff0f99f7cc9bbb232af63a077a480a3633bee1ef6\"\n },\n \"prevBlockHash\": {\n \"hex\": \"0000000000000000000000000000000000000000000000000000000000000000\"\n },\n \"work\": {\n \"hex\": \"14d4490000000000000000000000000000000000000000000000000000000000\"\n }\n }\n}\n"]
ret 0
output ["0\n"]
Result: 0
Thunder
Parent Chain
Coins
Mempool Explorer
Block Explorer
Withdrawals
Console / Logs
Transfer
Info
Deposit
amount
BTC
Fee
BTC
deposit
Withdrawal
mainchain address
generate
amount
BTC
fee
BTC
mainchain fee
BTC
withdraw
Balance: $0
Block height: 0 Best hash: 00000008...
Mine / Refresh Block
Bitcoin Core - ok - [signet]
File
Settings
Window
Help
Overview
Send
Receive
Transactions
This is a pre-release test build - use at your own risk - do not use for mining or merchant applications
Balances
Available:
0.00000000 BTC
Pending:
0.00000000 BTC
Total:
0.00000000 BTC
Recent transactions
Connecting to peers...
4 years and 9 weeks behind
BTC HD
cusf_launcher
Overview
Wallets
Tools
Settings
Layer 1 Software:
Bitcoin: Ready!
GRPCURL: Ready!
Enforcer: Ready!
Configuration: Complete!
BTC Running!
Drivechain Enforcer Running!
Layer 2 Software:
Thunder: Ready!
Thunder running!
Blocks: 0
Last Block: ? minutes ago
Peers: 0
Connections: Bitcoin:
CUSF Client:
Wallet:

CUSF

Core Untouched Soft Fork
"Ordinal-ization" of Soft Forks
(The Solution to everyone's problems)

Part 2 of 3

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

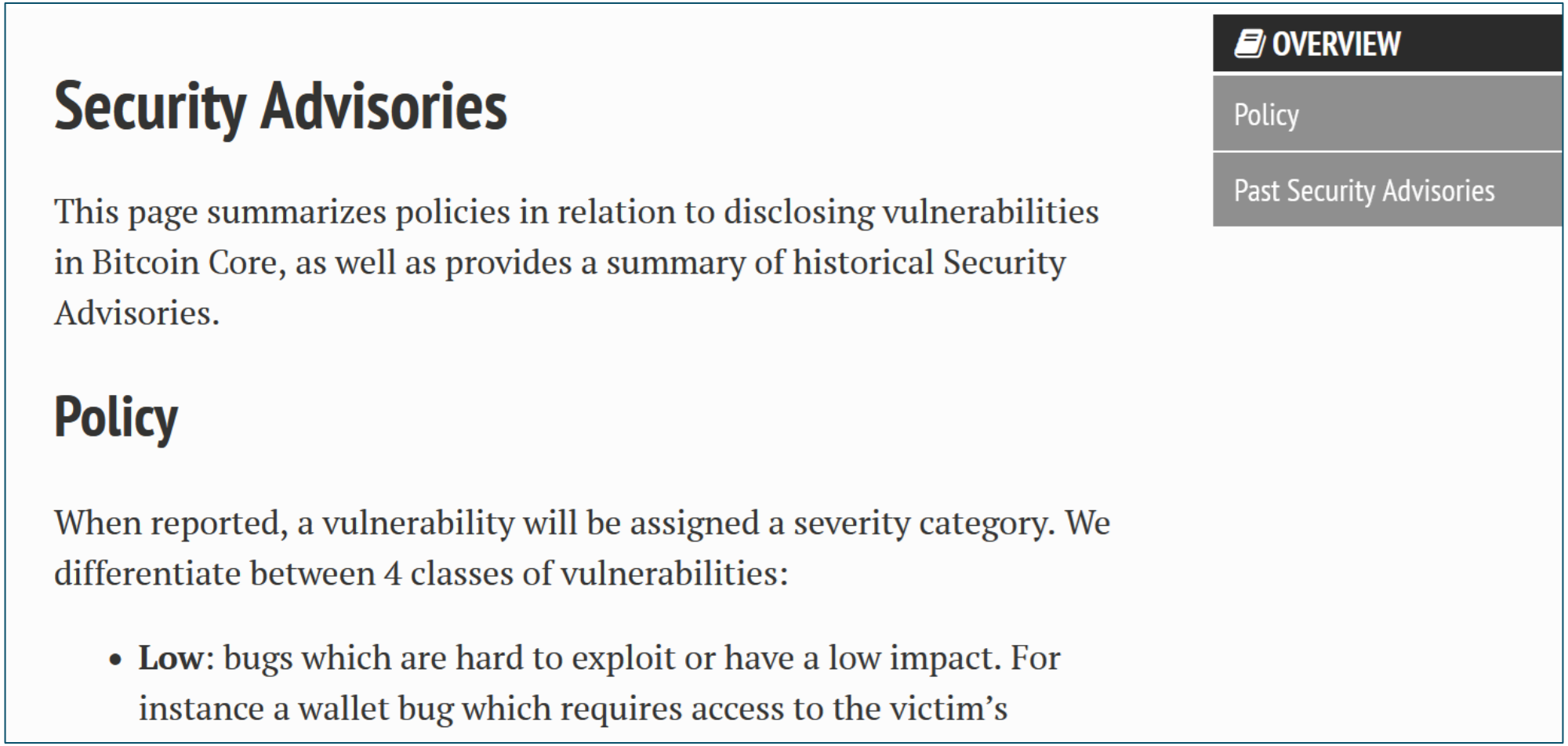
- SegWit
  - Announced Dec 2015
  - Coded Oct 2016
  - Activated Aug 2017

20 Months

- Taproot
  - Announced Jan 2018
  - Coded Oct 2020
  - Activated Nov 2021

46 Months

Roadblock 2: You can’t leave.



OVERVIEW

Policy

Past Security Advisories

Security Advisories

This page summarizes policies in relation to disclosing vulnerabilities in Bitcoin Core, as well as provides a summary of historical Security Advisories.

Policy

When reported, a vulnerability will be assigned a severity category. We differentiate between 4 classes of vulnerabilities:

- **Low**: bugs which are hard to exploit or have a low impact. For instance a wallet bug which requires access to the victim’s

Two Roadblocks

1. Bitcoin Core doesn't work anymore – (for soft forks).
2. You can't *leave* Bitcoin Core.

Solution: Keep Core unchanged – add a 2nd "activator" software.

- Takes blocks from Bitcoin Core, and gives them a "second pass".
- Calls `invalidateblock` in Bitcoin Core if new rulebreaking.

Benefits:

- Faster
- Safer
- Easier to Understand

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

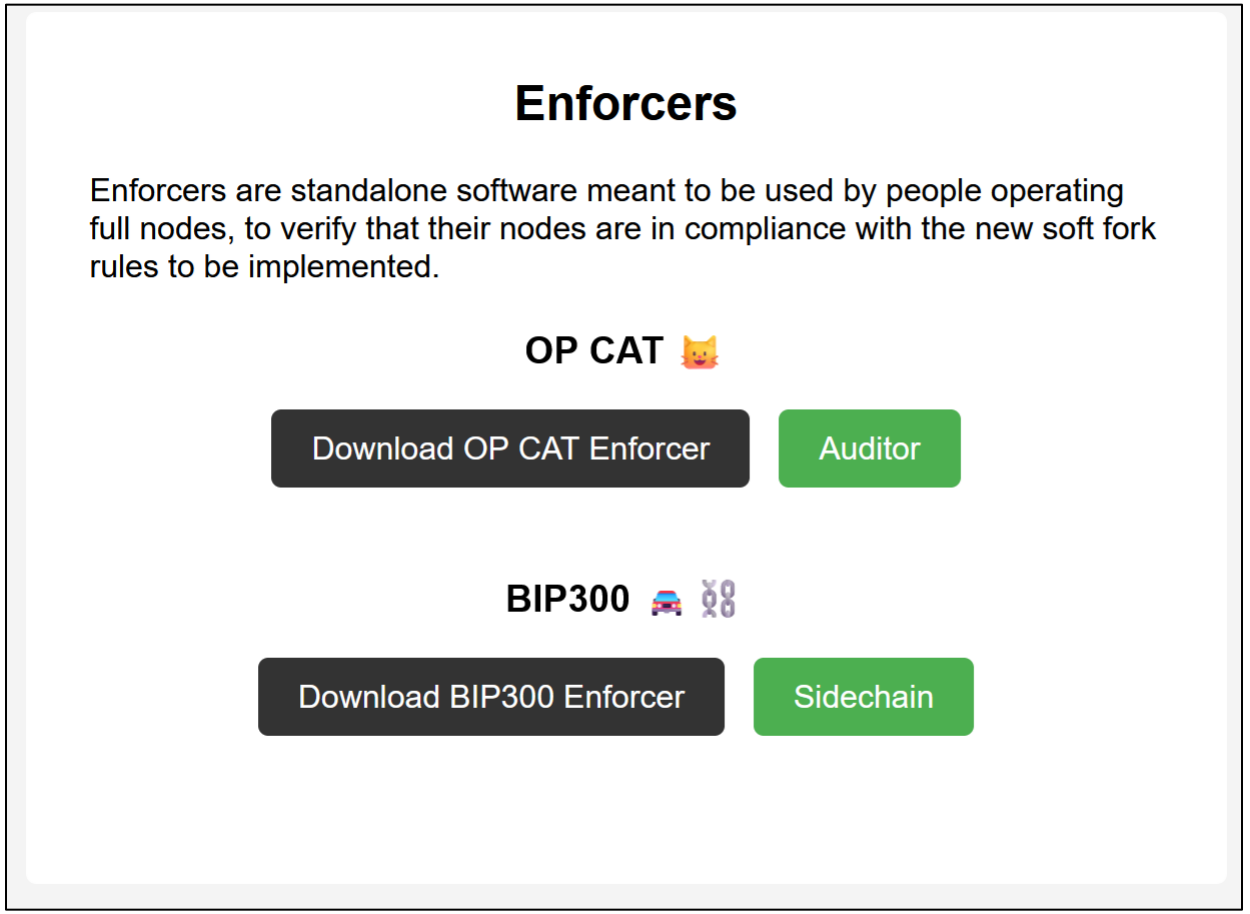
Each new soft fork (SF) should be a separate, standalone piece of software, "piloting" Bitcoin Core via the "invalidateblock" rpc. This makes soft forks *faster, safer, and easier to understand* -- ushering in a new age of Bitcoin Development.

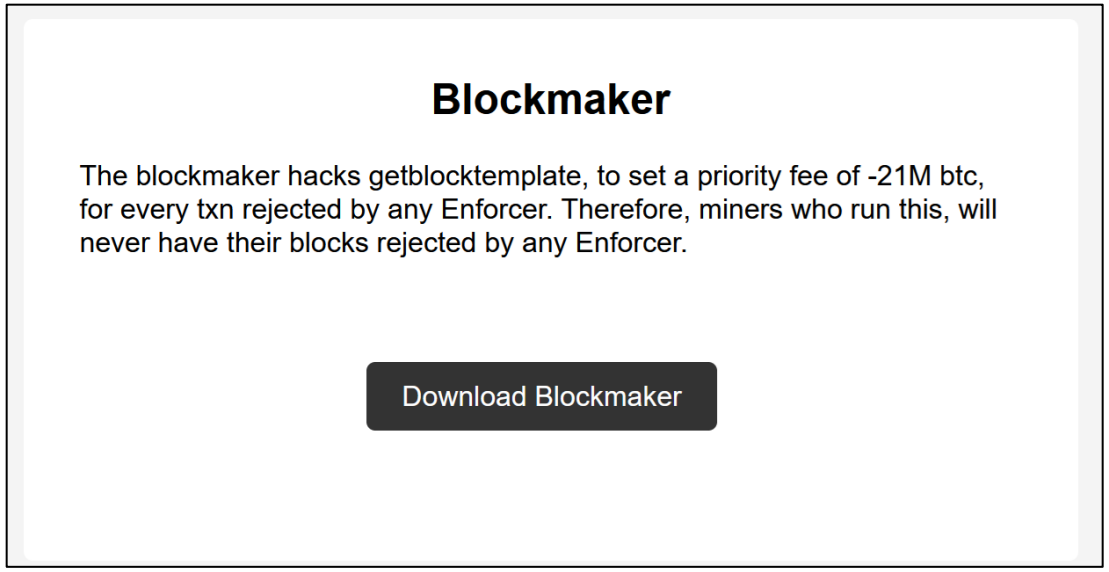
The Idea

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

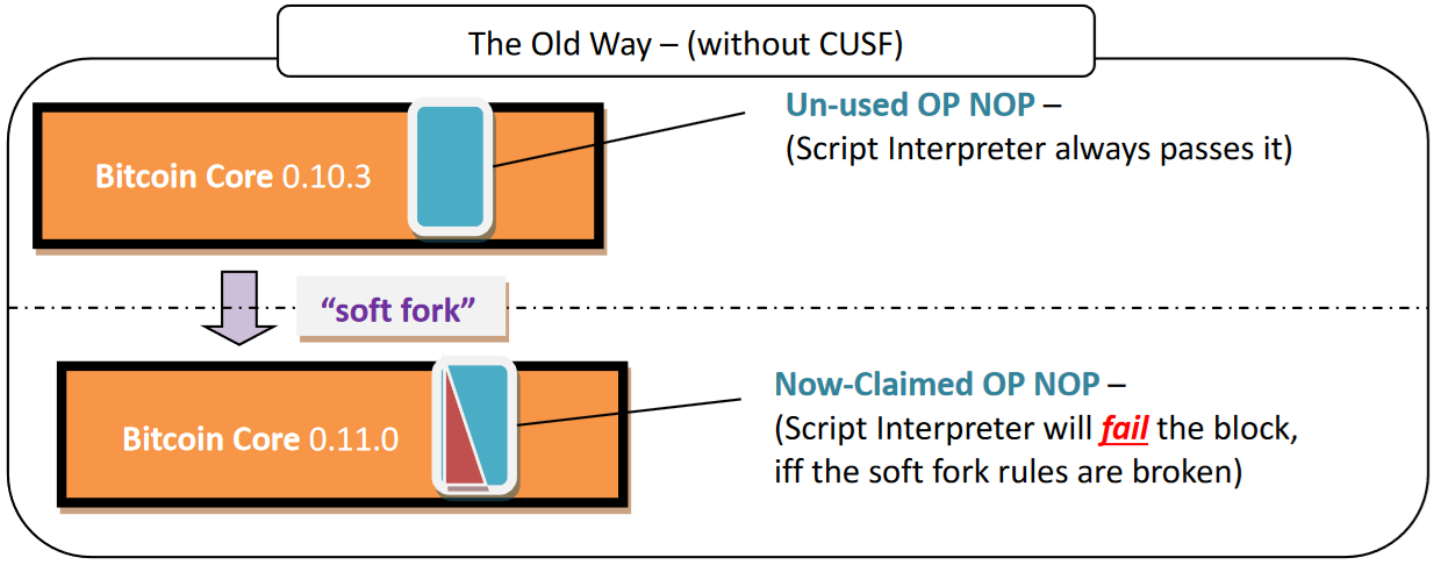
Download Today – OP CAT & BIP300

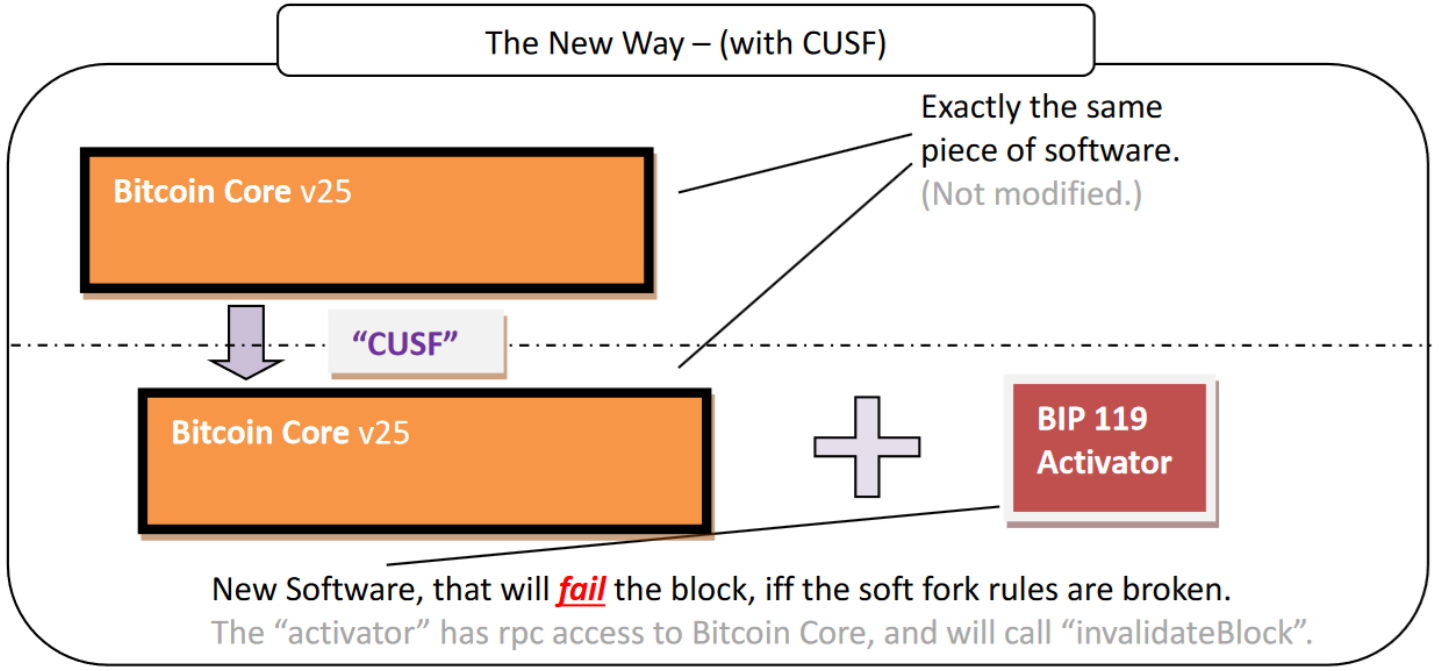




bip300cusf.com/download

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





- 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

My Proposal Is...

1. Miners run the Bip300 CUSF activator,
   (Bitcoin Core continues to do nothing).

2. Once 51% hashrate runs the CUSF addon, Bip300 activates.

3. Miners activate the Mined-L2s, (13-13) and collect $$ from them.

Problem solved!
(Bitcoin gets scalability & privacy &
extensibility & security budget & ossification)

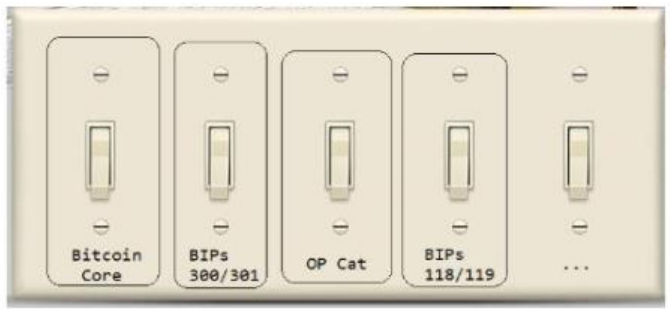
The Alternative Plan

- Take the same people, who for years were *overoptimistic* about the viability of Lightning…
- …give them money, & wait *more years*, for them to finish ARK….
- …something that is *way worse*, for the user, for no reason (more interactivity requirements, a liquidity rental cost, more complexity)…
- …something which *may not work at all* (which is very likely, given the track record of LN, CoinPool, channel factories)…
- …such that, even if it did work, miners would get *none of the money* , leading to conflict , eventual vertical integration, and MEV off-the-charts (as miners pursue their self-interest, of fee-collection)…
- …leading to a total *collapse of the original security model* anyway (which is of course not designed to withstand Miners-as-sole counterparty), making all the tech effort pointless…

The Alternative Plan

- Take the same people, who for years were *overoptimistic* about the viability of Lightning…
- …give them money, & wait *more years*, for them to finish ARK….
- …something that is *way worse*, for the user, for no reason (more interactivity requirements, a liquidity rental cost, more complexity)…
- …something which *may not work at all* (which is very likely, given the track record of LN, CoinPool, channel factories)…
- …such that, even if it did work, miners would get *none of the money* , leading to conflict , eventual vertical integration, and MEV off-the-charts (as miners pursue their self-interest, of fee-collection)…
- …leading to a total *collapse of the original security model* anyway (which is of course not designed to withstand Miners-as-sole counterparty), making all the tech effort pointless…
- …with the added risk that, if it takes too long to implement, then *the whole Bitcoin project might be replaced* , and fail and go to zero.

More About CUSF

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

	Before CUSF	After CUSF
How are SFs activated?	Follow these steps: 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.	Follow these steps: 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.

	Before CUSF	**After CUSF**
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 1st 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 justified to the layperson?	We need *to explain to people* why the SF is safe.	It is *obvious* that SFs are safe. No existing users can even *detect* 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 *increase miner profits?*

	Before CUSF	After CUSF
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 *choose* 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 *against* each other – (competition keeps developers honest). Developers are accountable to *a neutral external metric* (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.

	Before CUSF	After CUSF
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 *any* 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 *voluntarily consult* 3rd party expert advisors, and *choose* 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 3rd parties have a veto.

Yet More Slides

Conflicts of Interest

People's reputation, business model riding on various projects, so -- consciously or not, they will be biased in their assessment.

	Miners	Investors	Developers	Users
Miners		**Liquidity-vs-Illiquidity** **Hype-vs-Substance** **Volatility-vs-Stability**	**Non-mined L2s (LN, ARK, BitVM, Liquid) / "middlemen schemes" (taking fees from miners).** vs **Merged Mining**	**High Total Fees** vs **Low $/txn feerate**
Investors		**-**	**Developer "Pet Project" Lock-In, Monopolist Guilds,** vs **Improving Coin Competitiveness**	**Number Go Up** vs **Day to Day Usage**
Developers			**-**	**Complex Impressive Whitepapers, Backends** vs **Great UX, Nice Features, Frontends**
Users				

“Motivation to Adopt” a Soft Fork

Analyzing Bitcoin Consensus: Risks in Protocol Upgrades

Ren Crypto Fish* Steve Lee† Lyn Alden‡

November 2024

Abstract

Table 3 – continued from previous page

Stakeholder	Motivation to adopt	Motivation against adopting
Users and Application Developers	• Enhanced capabilities or functionality that might support more advanced or scalable applications • Incentives to build on a protocol with more flexible or innovative transac-	• Risk of incompatibility with existing applications or services leading to potential loss of user funds • Uncertainty over stability, maintenance, and security of the alternative

“Motivation to Adopt” a Soft Fork

Analyzing Bitcoin Consensus: Risks in Protocol Upgrades

Ren Crypto Fish* Steve Lee† Lyn Alden‡

November 2024

Full Throttle Innovation + Adoption

Complacency & Laziness

Stakeholder	Motivation to adopt	Motivation against adopting
Users and Application Developers		

Bitcoin Survives

→ 15 M$/coin

→ X00 B $/year fees

Bitcoin Dies

(something else becomes global money)

Btc price & fees → 0

Problem

Innovation & adoption will either make, or break, BTC.

Innovation

- Innovation *created* Bitcoin – so, it could create something better, any day now!
- Innovation is *unpredictable* – no one predicted the invention of Bitcoin ...the next great idea will also be a surprise.
- ... is *hard to assess*. For every genius inventor, there are 500 frauds and cranks.
- ... is always a *risk*. Every improvement is a *change* – it could therefore, instead be a mistake, an attack vector, or sabotage.
- ... is always a *dissent* from a prevailing orthodoxy. Most cypherpunks / Austrians hated Bitcoin at first – all *good new ideas* will be hated by Bitcoiners at first.
- ... always *reorders status* in a community. Better scaling would put Lightning out of business, better privacy would put CoinJoin out of business, improved self-custody would put BitGo out of business. Better UX puts educators out of business, etc. These are natural *enemies of innovation*. Innovation *never has consensus*.

Adoption

Blockchain tech is improving fast.

- 99% of new projects are scams – but this has blinded people to the true pace of progress.
- In 3-5 years, it will be possible for *anyone* to launch a new coin that is [1] globally scalable, [2] fully private, [3] capable of replacing fiat payment systems, all on [4] layperson hardware/internet.
- After that, only network effects will matter. Whichever coin *innovates most on adoption* will then win.
- Soon (probably by 2035), only one currency will remain. **BTC will either go to $200T, or $0.**

The Hubris of Complacency

- "[Easter Islanders] may have arrived on the island as early as the fifth century CE. They developed a complex Stone Age civilization, which suddenly collapsed over a millennium later. By some accounts there was starvation, war and perhaps cannibalism. The population fell to a small fraction of what it had been, and their culture was lost.

  The prevailing theory is that the Easter Islanders brought disaster upon themselves, in part by chopping down the forest which had originally covered most of the island. They eliminated the most useful species of tree altogether.

  …

  Of the hundreds of statues on the island, built over the course of several centuries, fewer than half are at their intended destinations. The rest, including the largest, are in various stages of completion, with as many as 10% already in transit on specially built roads. Again there are conflicting explanations, but, according to the prevailing theory, it is because there was a large increase in the rate of statue-building just before it stopped for ever. In other words, as disaster loomed, the islanders diverted ever more effort not into addressing the problem – for they did not know how to do that – but into making ever more and bigger (but very rarely better) monuments to their ancestors. And what were those roads made of? Trees."

  -David Deutsch, *The Beginning of Infinity*

"Wrong Solution" Feedback Loop

More Problems → More Statues

Things Which Are Inevitable

- Planetary Scale Tech Stack – one cryptocurrency will be able to process trillion txns/year. This has already happened – theory in 2021 and is happening now in practice.
- Coins Adopt This Tech Stack – Desperate for market share / selling points, Altcoins will install this tech stack.
- Pro-Adoption Coin Takes Over – One coin will prioritize adoption, and it will slowly gain network effect. Will hit various “critical mass” points and achieve super-exponential growth.
- That coin will process all the world’s txns – x trillion, $0.10 /txn, their miners will collect X00 B per year, growing 6% per year.
- Probably, all other coins will die off at that point.

Soft Forks Basics/History

Part 1 of 4

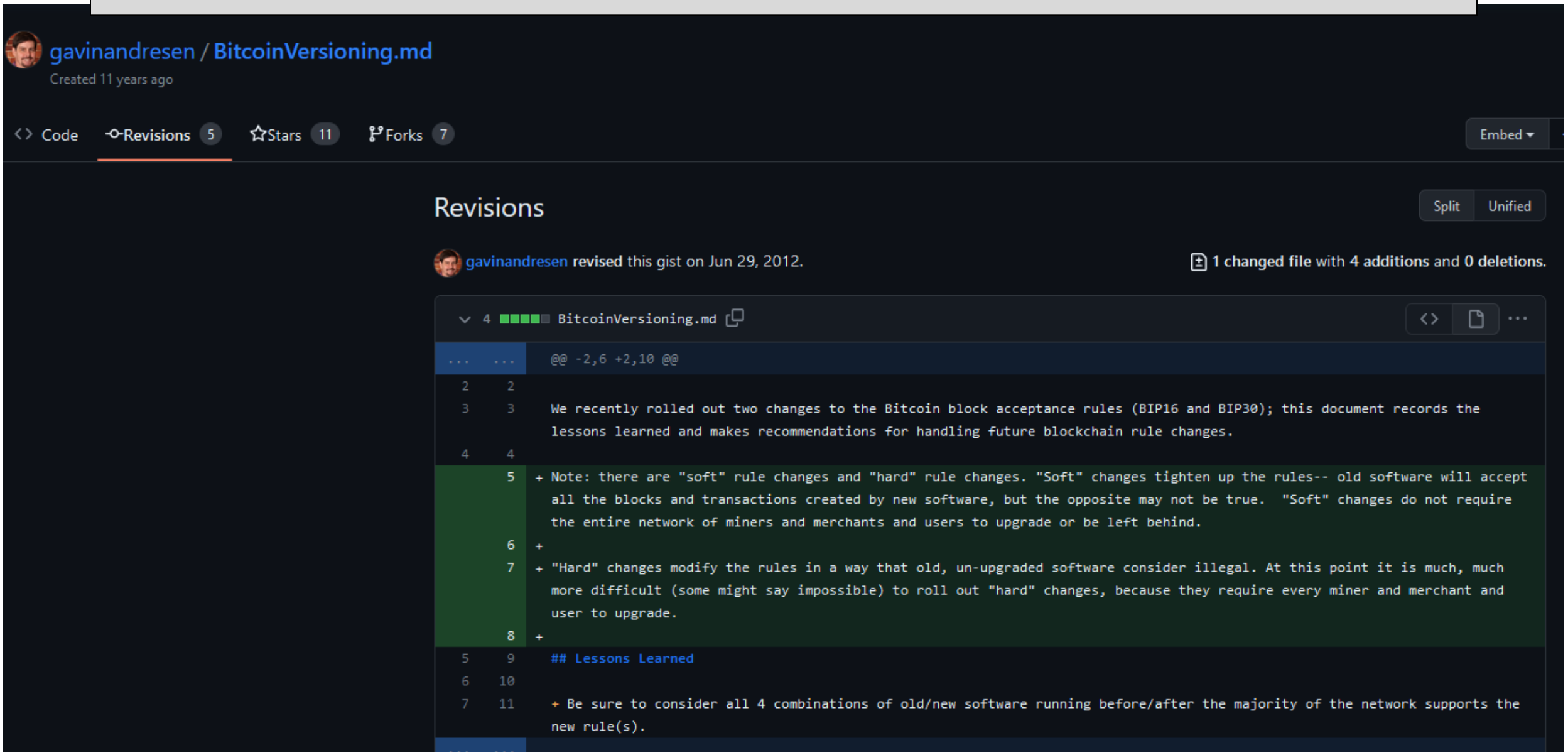
Soft Forks – The Basics

- 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)

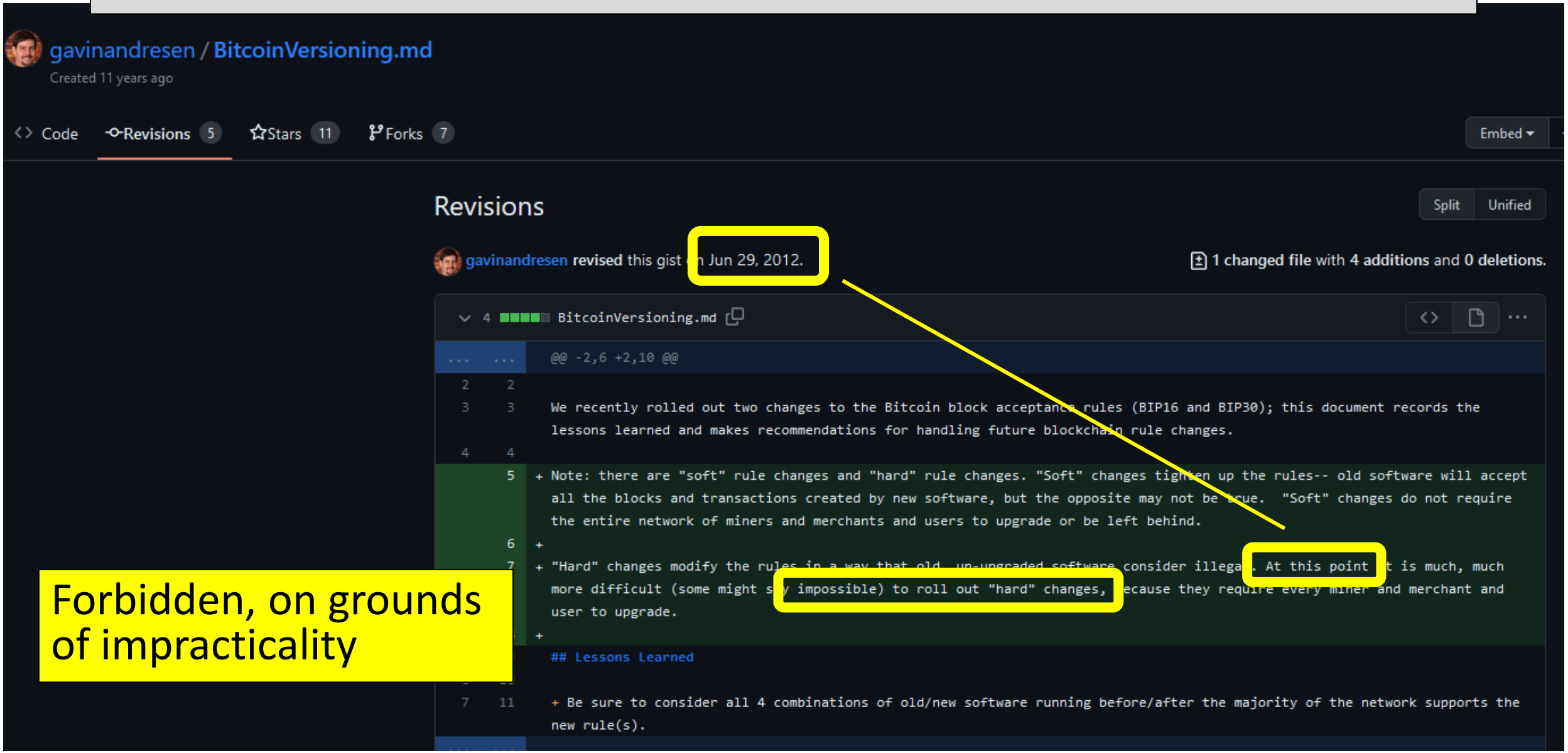
Some History – Not Widely Known

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”



Gavin Called them “Soft Changes”



Forbidden, on grounds of impracticality

In Blockchain, Fork Has a Strange Meaning

Culinary Fork?

Yes

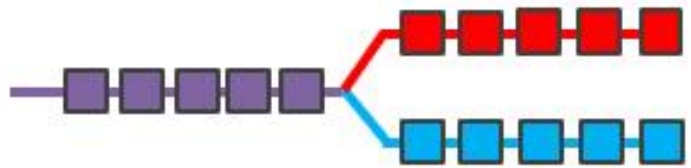
Tuning Fork?

Yes

Fork in the Road?

Yes

Blockchain (hard/soft) Fork?



No!

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

Nov 2012 – Definitions

Welcome, **Guest**. Please login or register.

News: Latest Bitcoin Core release: 24.0.1 [Torrent]

HOME | HELP | SEARCH | LOGIN | REGISTER | MORE

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)

[+] jcoinner 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

Governance – Definition

- Rejects P2P

Governance – Definition

- 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 Coexistance" 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

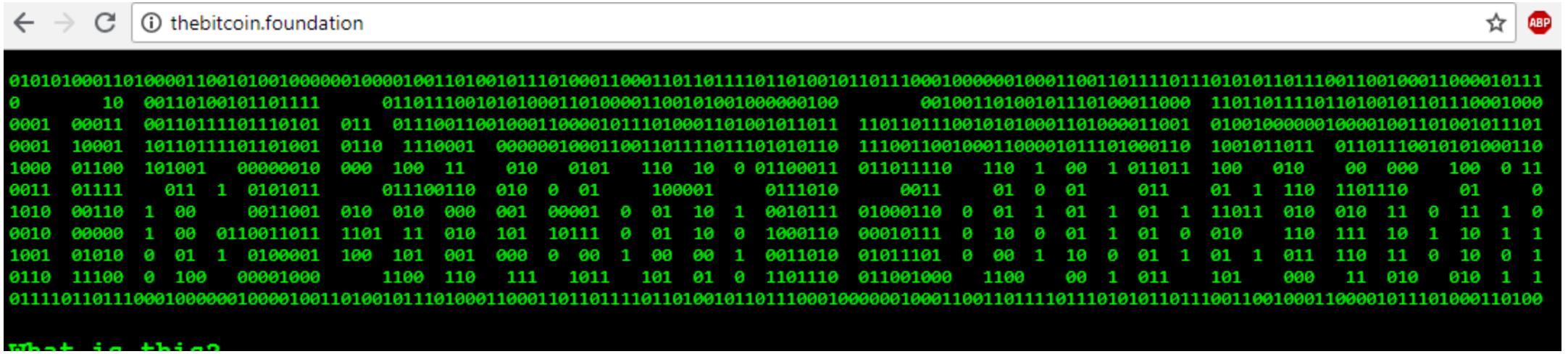
1. **Go to Bitcoin.org and Run The Latest Version**
    1. Luke Dashjr Position
    2. Mike Hearn position as well!
    3. Satoshi's position, (?) repudiated when he removed OP VER.
2. **Find the oldest node-like thing, run that, then plug your ears!**
    1. Never revisit this process. The relative 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 Coexistance" is fair game!

"Latest Core"

"Static" Protocol

"Linear Coexistence" (Consent-Based)

The “Static Protocol” Position



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 Coexistance" is fair game!

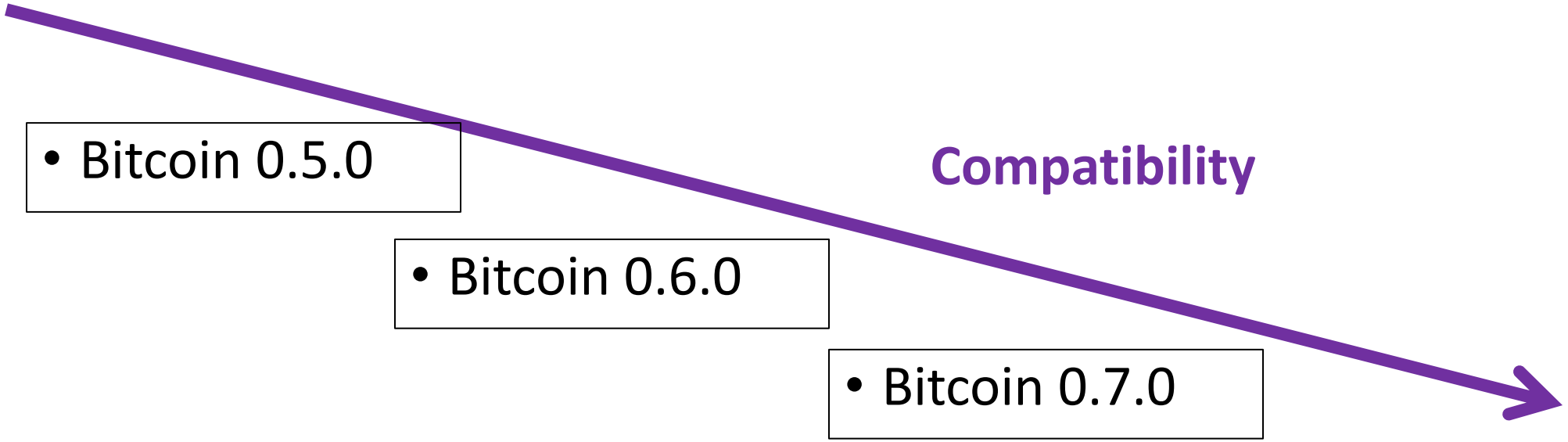
"Latest Core"

"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 Coexistance" 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	

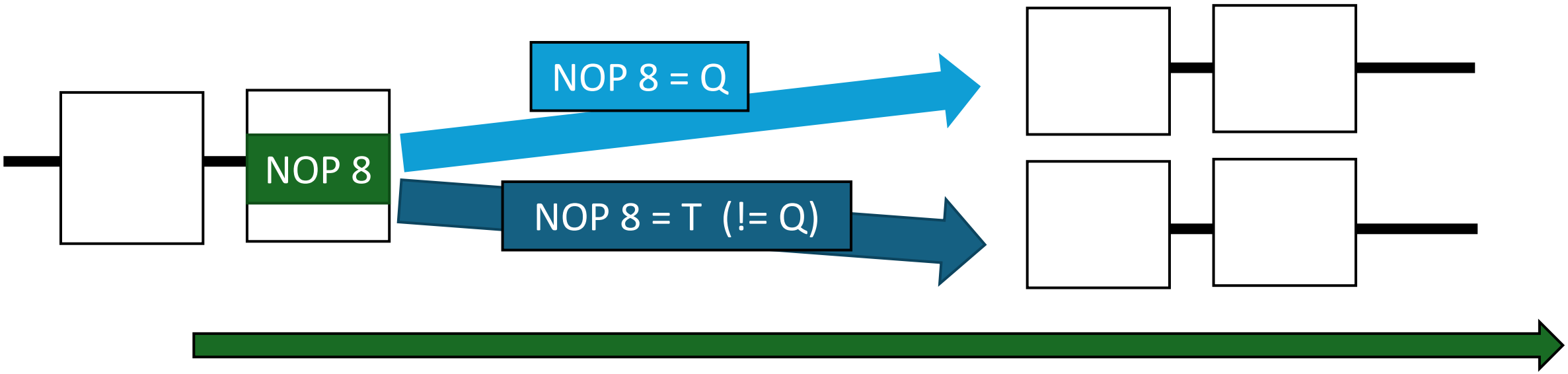
Expertise... is Mandatory!

- 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

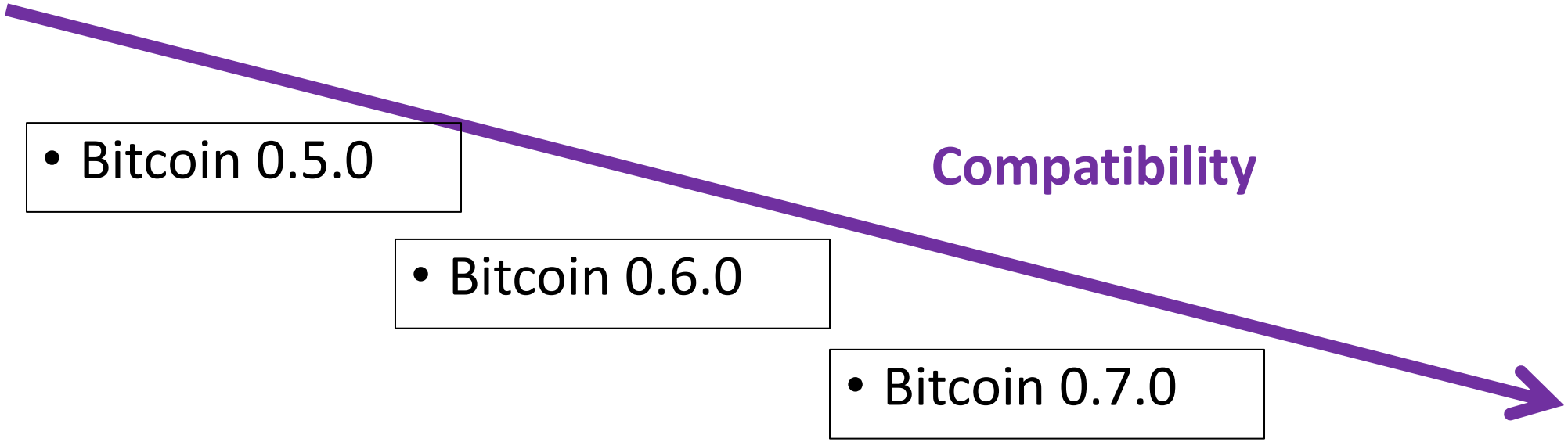
	Problem of Expertise / Charisma Attack	Outsourced Thinking / Fallibilism	Problem of Innovation / "Dissent"
"Latest Core"	No Laypeople Allowed	Outsource Your Thinking to Bitcoin.org	
"Static" Protocol	Accumulates Trust	Stays the Same	
"Linear Coexistence" (Consent-Based)	Requires dispute-resolution	Allows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

Two Incompatible SFs at once = HF



Upgrading via Soft Fork

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



Must be in order!

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				
	2015	Qtr1				
		Qtr2				Gavin's last Github merge.
"Scaling Bitcoin" Era		Qtr3		1		DER sigs required.
		Qtr4		1		Add CLTV.
	2016	Qtr1				
		Qtr2				
		Qtr3		3		Add rLT, CLTV, and enforce median-time-past.
		Qtr4				3rd SB Conference, SegWit blockade begins.
UASF Era	2017	Qtr1				
		Qtr2				
		Qtr3			1	SegWit Activated.
		Qtr4				SegWit2x Fork Abandoned, Rise of BCH.
LN Era / Fork Era (?)	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.

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....

The Real Reason...

gavi
Create

Code

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 @@

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.

+ 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.
+
+ "Hard" changes modify the rules in a way that old, un-upgraded software consider illega. At this point t 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

+ 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