

Consensus and Dissent

or: “Meta-Consensus” – “Consensus about
what we have consensus on”

Building on Bitcoin
Lisboa, Portugal -- 4 July 2018



Paul Sztorc
Twitter: @truthcoin
paul@tierion.com

Agenda

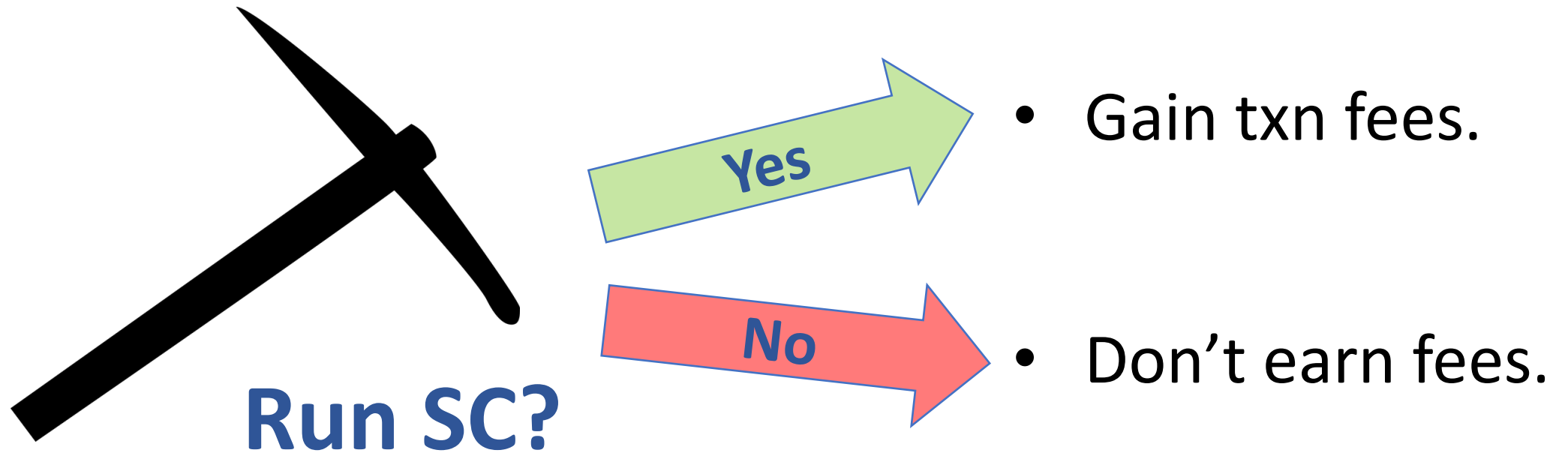
1. Two Sidechain Philosophies
2. The Soft Fork, and Bitcoin's Ongoing Identity Crisis

Belief #1

“Sidechains affect the [mainchain] miners.”

- (Explanation – next slide)
- Implies that:
 - SCs are not a true “layer-2”.
 - SC-censorship is justified.
- Important because: last trench of the anti-SC-er.

“Sidechains affect the miners”



1. SCs offer a conditional payment to miners,
2. Miners have no choice but to accept,
3. The conditions are bad for Bitcoin.

Ergo: SCs are bad for Bitcoin.

Belief #2

“Sidechains allow miners to steal BTC.”

- Implies that:
 - Users may be “tricked” into losing coins.
 - Security is different. Moves from “math based” to “incentive based”.
- Important because:
 - Justifies Tx-censorship. (Must “””protect””” user.)

Do they contradict?

Belief #1

SCs affect miners.

- SCs → miners.
- Miners are **weak**, pliable.

Belief #2

SCs enable miner-theft.

- Miners → SCs.
- Miners are **strong**, do the plying.



Do they ~~contradict~~?

Belief #1

Anything could...

~~\$s~~ affect
miners.

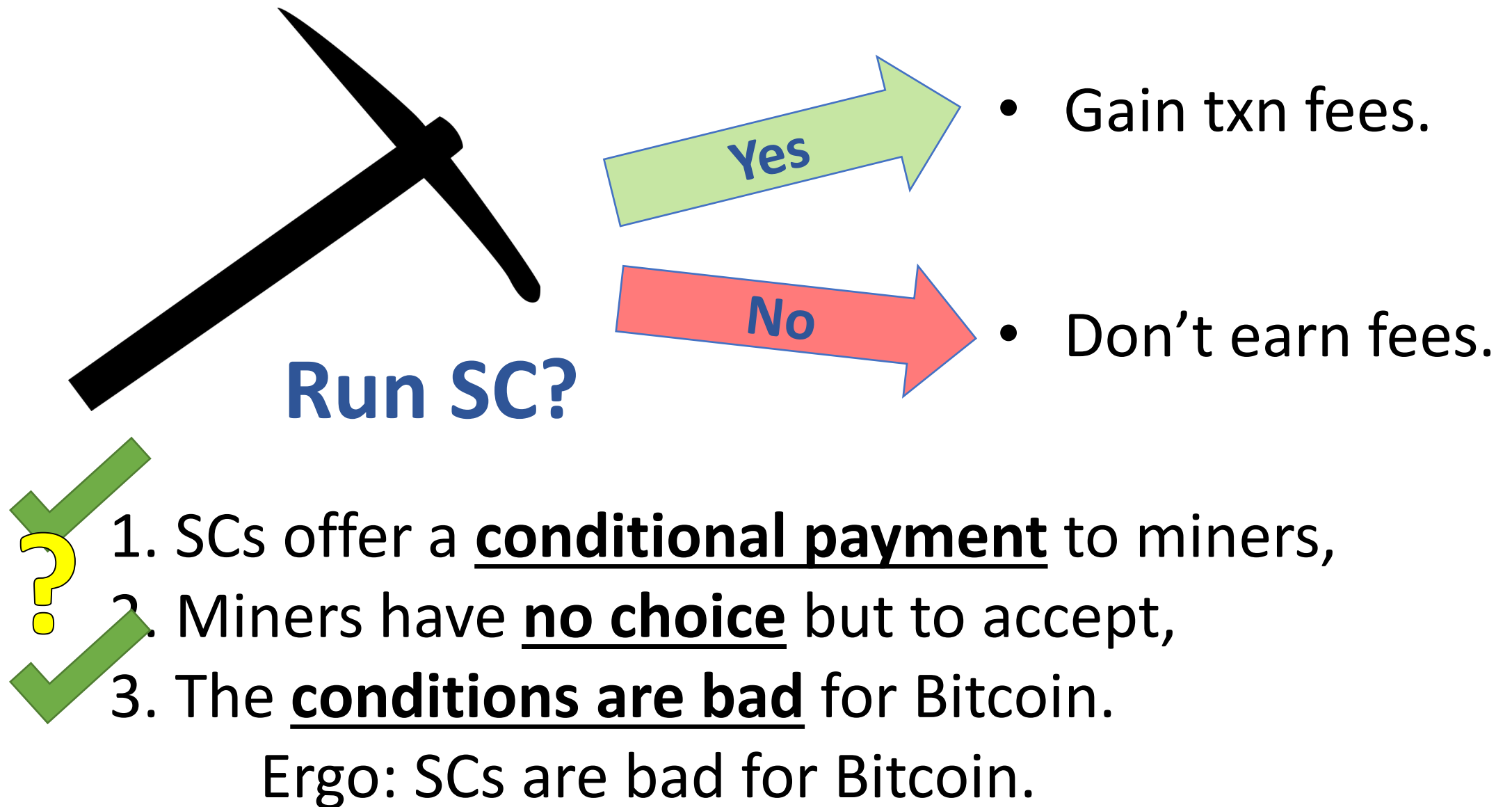
Belief #2

Everything [txn]...

~~\$s~~ enable
miner-theft.

(Theft has always
been “enabled”.)

“Sidechains affect the miners”



Chinese gov't affects the miners"

inducement

Reveal mailing
address?

Bad thing

Yes

- Gain **1 BTC**

No

- Don't earn.

?

1. SCs offer **inducement**
2. Miners **who**
3. The **con** are

Ergo: SCs are bad for Bitcoin.

We will pay 1 BTC per month,
to any miner who
reveals their mailing address.

The US FED affects the miners"

inducement

Obtain mining
license?

Bad thing

Yes

- Gain 1 satoshi

No

- Don't earn.



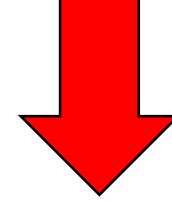
1. SCs offer condition
2. Mine cho
3. The c



Ergo. are bad for Bitcoin.

We will pay 1 satoshi per year,
to any miner who
obtains a mining license.

Belief #2

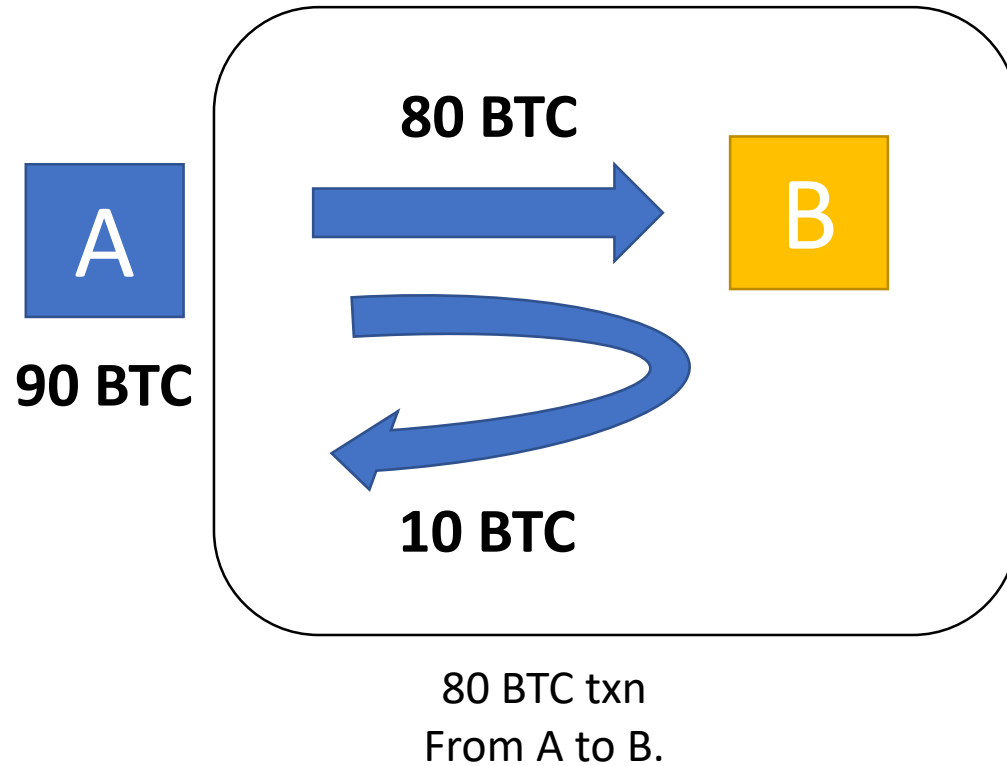


*“Sidechains ~~allow~~
miners to steal BTC.”*

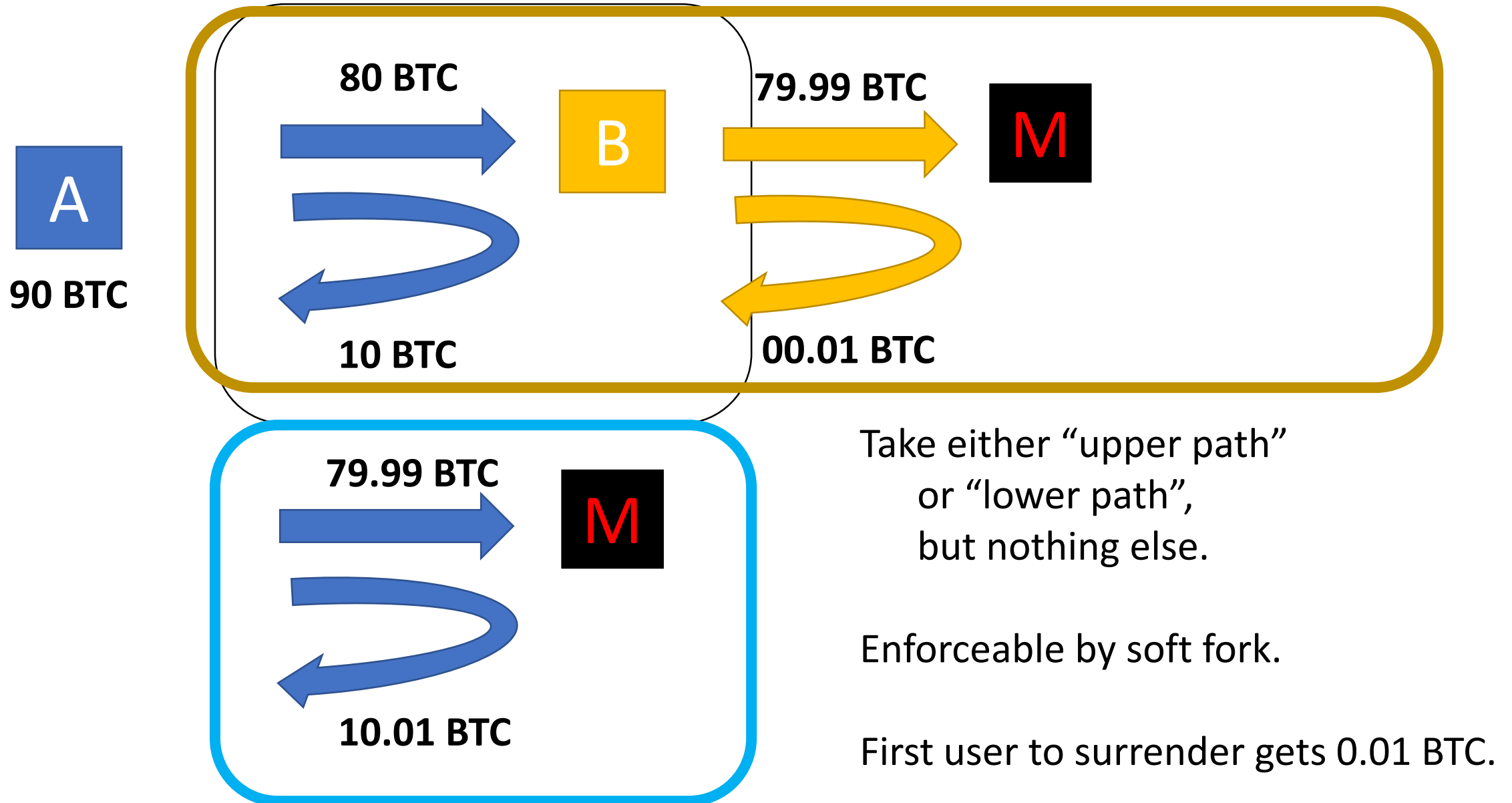
Hashrate majority can
steal from anything.

(SCs, mainnet, LN)
All have identical security assumptions.

“Hashrate majority can steal coins”



“Hashrate majority can steal coins”



“Hashrate majority can steal coins”



Blue says: “Let me broadcast tx1, and I will give you 18.99 of the 19.00 that I steal.”

Notice, though, if Yellow pays a 19 BTC txn fee, she is only left with 11 (instead of 28)

Yellow may be shaken down for the whole 30.

“He ought to find it more profitable...”

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

What does affect mainchain miners: Altcoins

[bitcoin-dev] Total fees have almost c

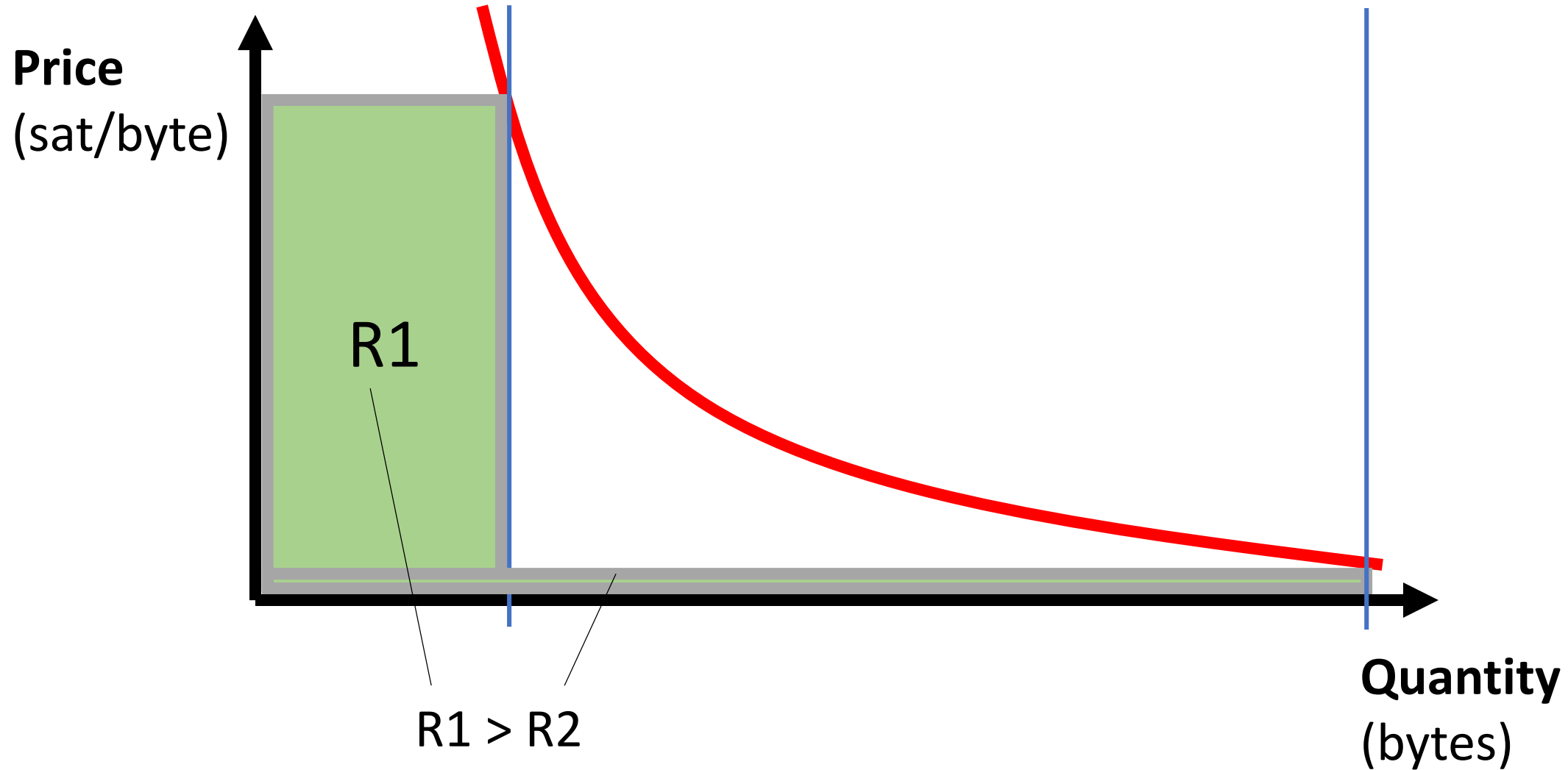
Gregory Maxwell [greg at xiph.org](mailto:greg@xiph.org).

Thu Dec 21 22:44:32 UTC 2017

- Previous message: [\[bitcoin-dev\] Total fees have almost crossed the block](#)
- Next message: [\[bitcoin-dev\] Total fees have almost crossed the block rev](#)
- **Messages sorted by:** [\[_date_\]](#) [\[_thread_\]](#) [\[_subject_\]](#) [\[_author_\]](#)

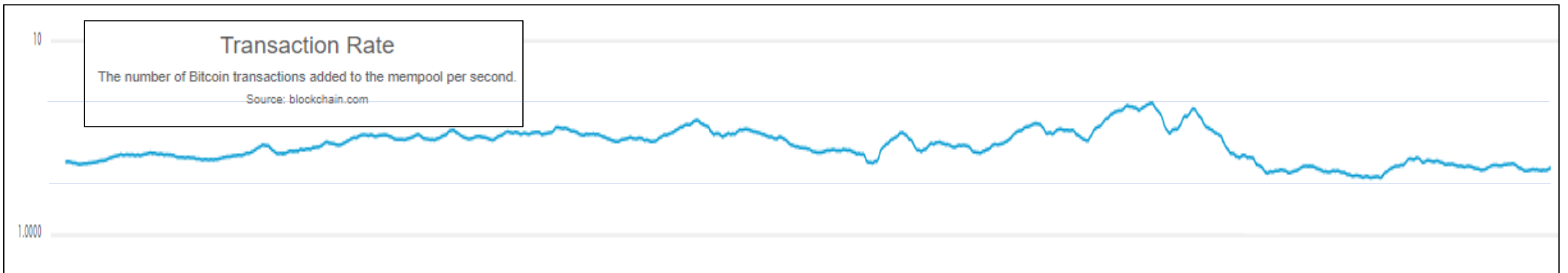
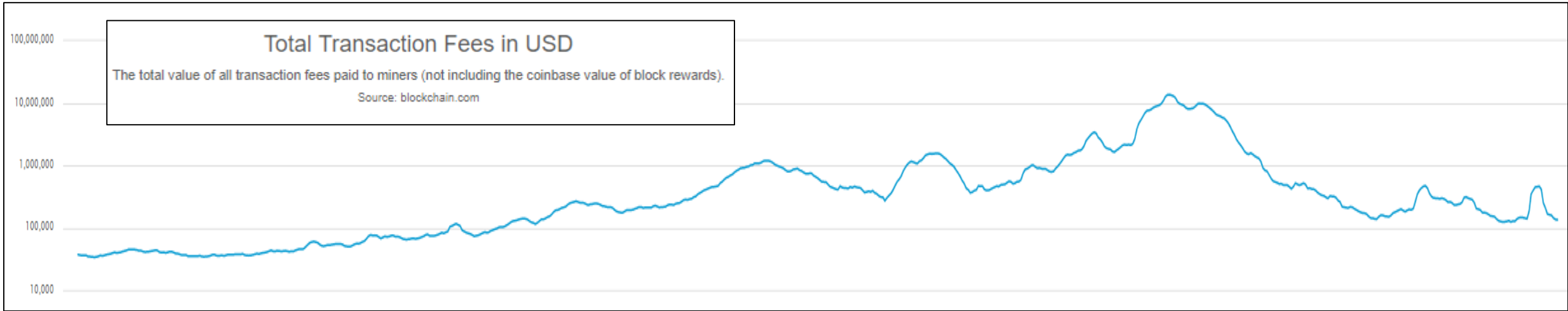
Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation, and also producing fee paying backlogs needed to stabilize consensus progress as the subsidy declines.

What does affect mainchain miners: Altcoins



High Fees → Less Usage

Last 2 Years, Log Scales, 7d average



Fee revenues are important...

[bitcoin-dev] Total fees have almost c

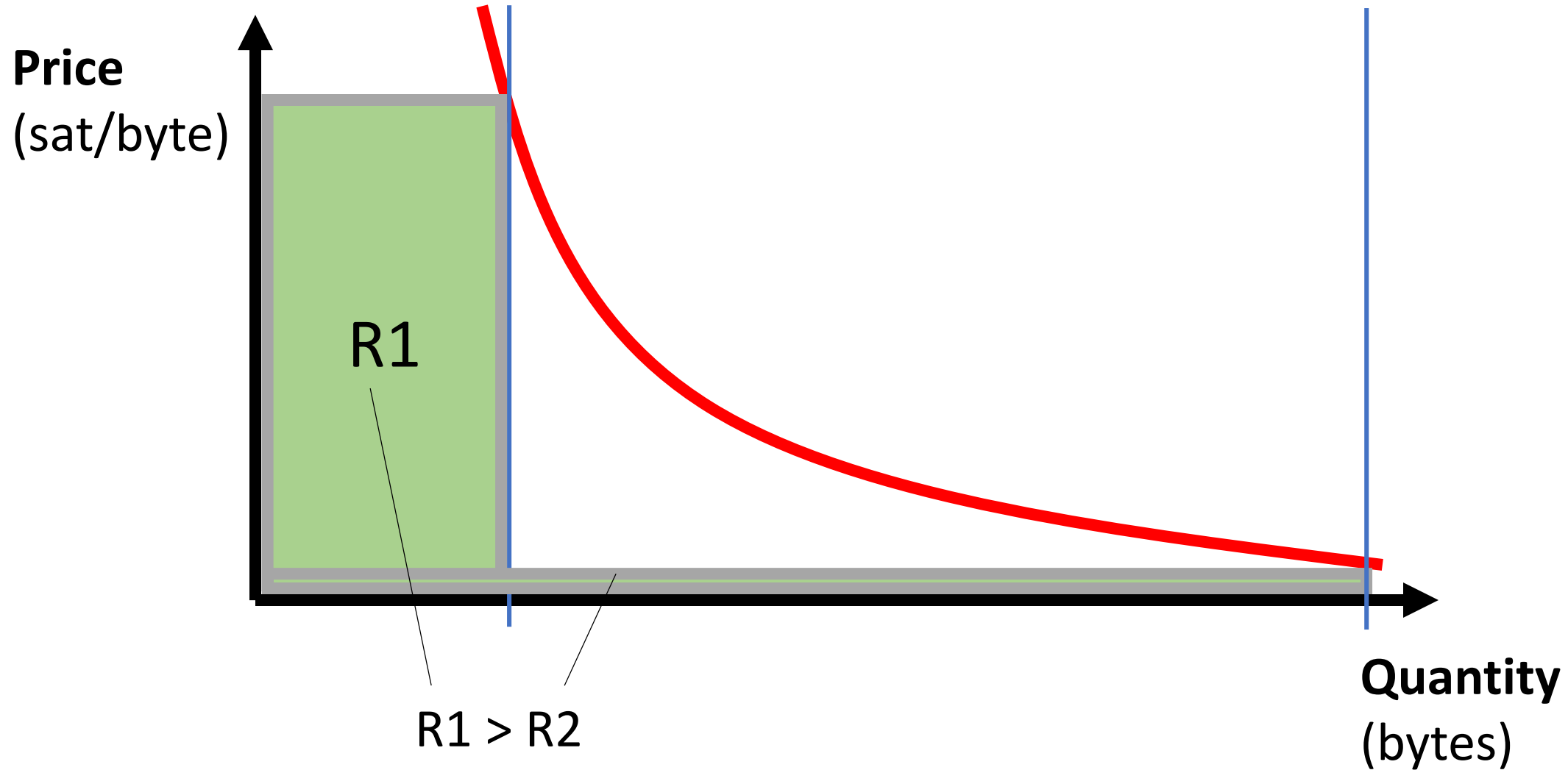
Gregory Maxwell [greg at xiph.org](mailto:greg@xiph.org).

Thu Dec 21 22:44:32 UTC 2017

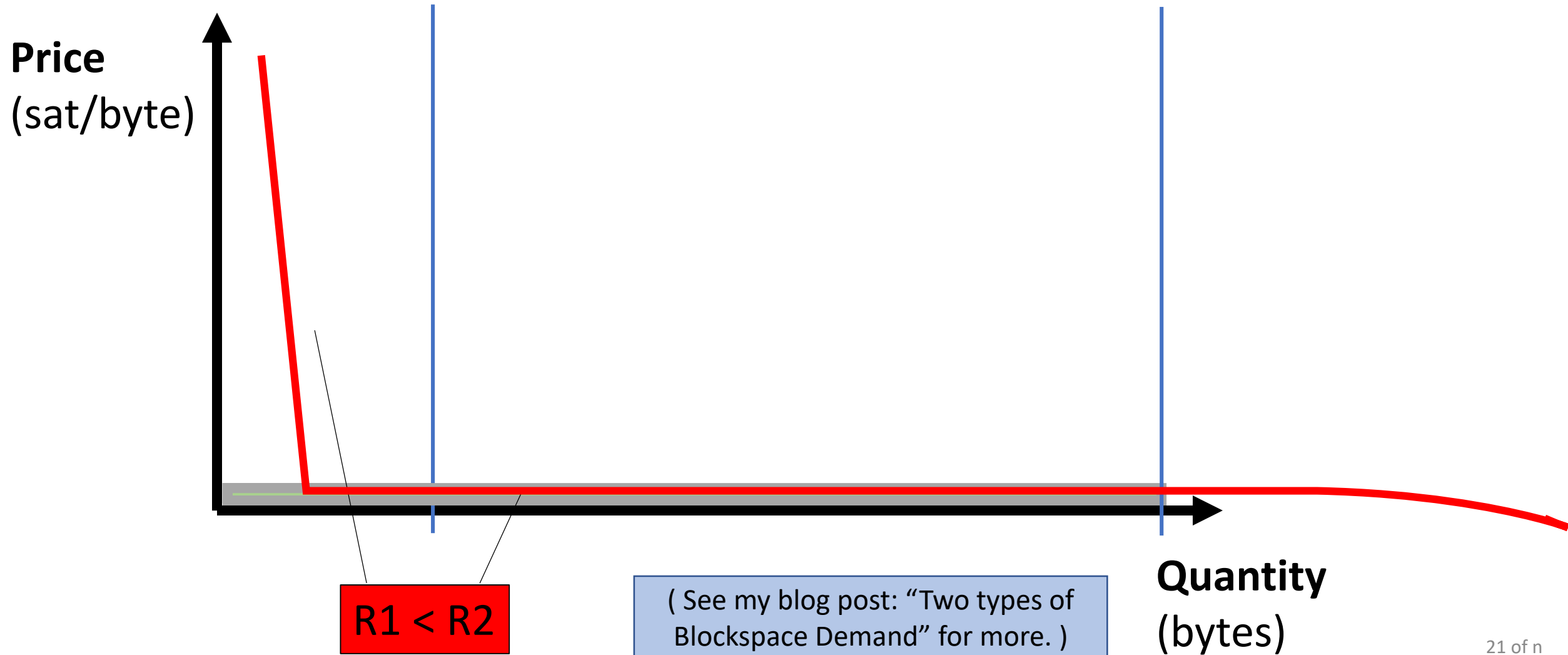
- Previous message: [\[bitcoin-dev\] Total fees have almost crossed the block](#)
- Next message: [\[bitcoin-dev\] Total fees have almost crossed the block rev](#)
- **Messages sorted by:** [\[_date \]](#) [\[_thread \]](#) [\[_subject \]](#) [\[_author \]](#)

Personally, I'm pulling out the champaign that market behaviour is indeed producing activity levels that can pay for security without inflation, and also producing fee paying backlogs needed to stabilize consensus progress as the subsidy declines.

...and supply affects Fee Revenues.



What does affect mainchain miners: Altcoins



Agenda

1. Two Sidechain Philosophies

2. The Soft Fork, and Bitcoin's Ongoing Identity Crisis

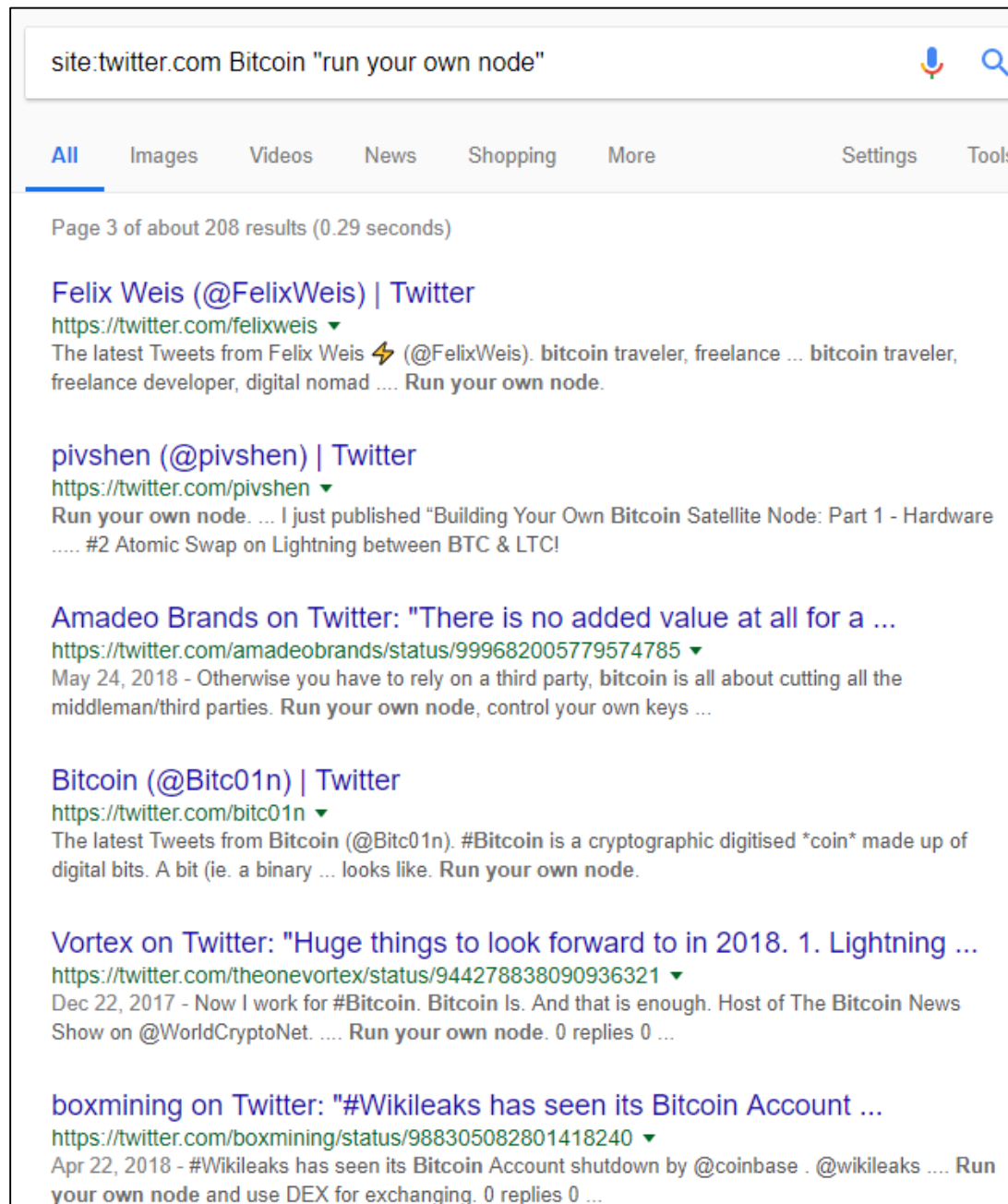
Consensus...About What?

- Bitcoiners sometimes disagree.
- Meta-Consensus – Consensus about consensus
(^^ it must be prior to Consensus itself)



Full Node Mandate

- Advice contains a little circular reasoning.
- How do we tell “a full node” from “NOT a full node”?



Wladimir Dictatorship / Vague Oligopoly (??)

Start Buy News FAQ Mining Alt-coins

Diff. 5.36t

Wladimir van der Laan - Lead Maintainer, Bitcoin Core

Wladimir van der Laan is a [Bitcoin Core](#) Developer and the Lead Maintainer of the Bitcoin repository on GitHub.

Bitcoin Core

From mid-2010 until April-2014, [Gavin Andresen](#) maintained control of the Bitcoin Core GitHub repository and was considered Bitcoin's lead developer. On April 8, 2014, Andresen stepped down and van der Laan agreed to take over as Lead Maintainer of the Bitcoin repo. His salary is paid by MIT's Digital Currency Initiative, where he works on Bitcoin development with Andresen and Cory Fields.

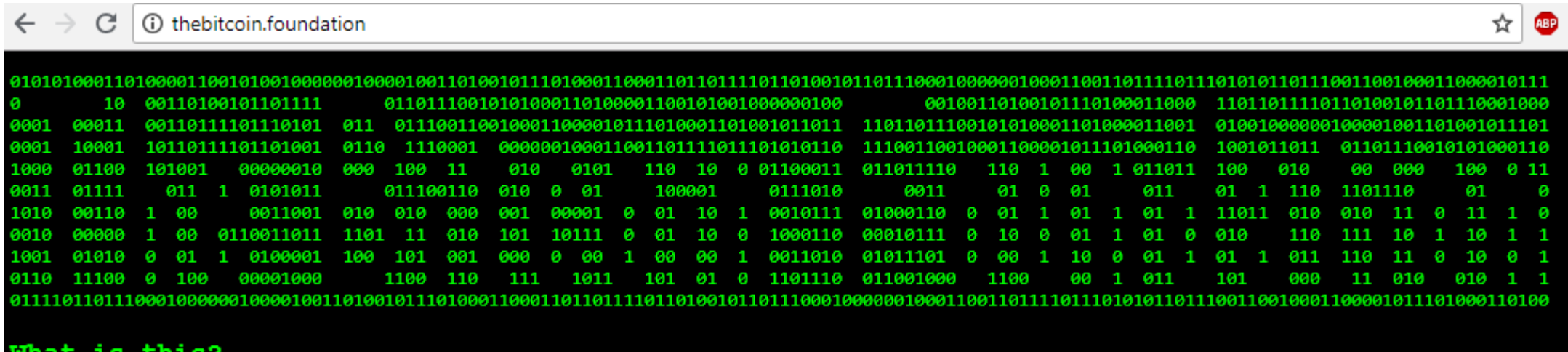


Position: Lead Maintainer, Bitcoin Core

Twitter: [@orionwl](#)

GitHub: [@laanwj](#)

The “Static Protocol” Position



01010100011010000110010100100000010000100110100101110100011000110110111011010010110111000100000010001100110111101110101011011100110011000010111
0 10 00110100101101111 01101110010101000110100001100101001000000100 00100110100101110100011000 11011011110110100101101110001000
0001 00011 00110111101110101 011 0111001100100011000010111010001101001011011 1101101110010101000110100011001 01001000000100001001101001011101
0001 10001 10110111101101001 0110 1110001 00000100011001110111011101010110 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
0111101101110001000000100001001101001011101000110001101101111011010010110111000100000010001100110111101101011011100110001100001011101000110100

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

The “Static Protocol” Position

← → ↻ thebitcoin.foundation

```
0101010001101000011001010010000001000010011010010111010001100011011011101101001011011100010000001000110011011110
0
0001 00011 00110100101101111 01101110010101000110100001100101001000000100 00100110100101110100011000
0001 00011 00110111101110101 011 0111001100100011000010111010001101001011011 1101101110010101000110100001100
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
100001011101000110100
```

I call this the “loudness” of the fork.
(See my blog post
“Better Fork Terminology” for more.)

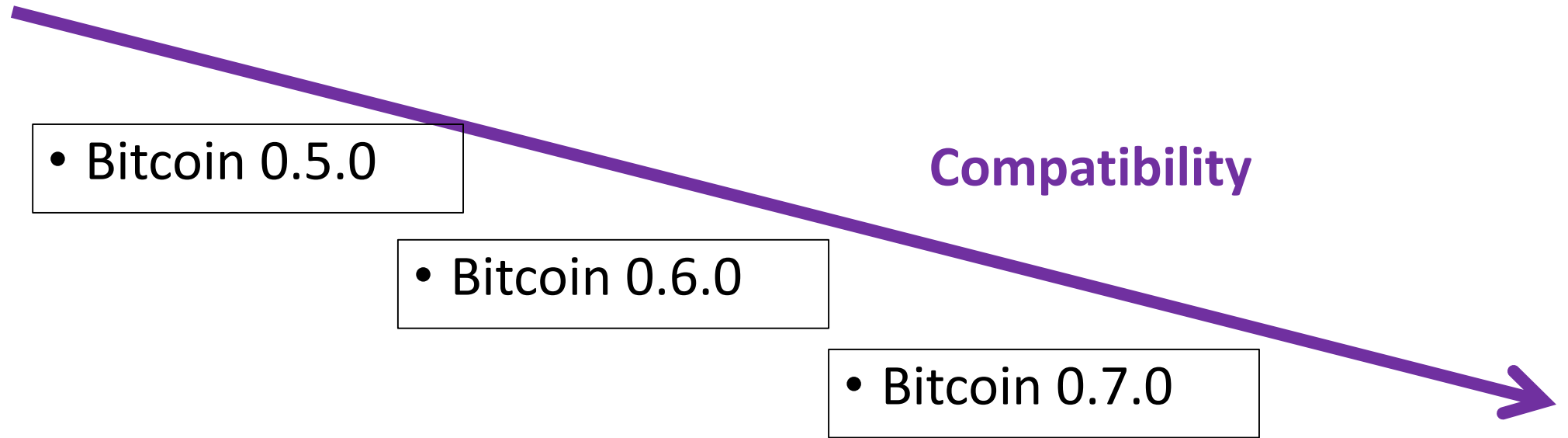
1. Clear Errors -- value overflow, spend other's BTC, and malleability.
2. Protocol can be unilaterally changed (MASF, UASF) -- then, payments made to you, might go "through" these "new txns".
3. Extremely Pessimistic -- Bitcoin can never improve, ever.
4. Stimulates creation of Altcoins / Hard Forks

use, copy or
it to anyone or
o continue doing
erify any PGP

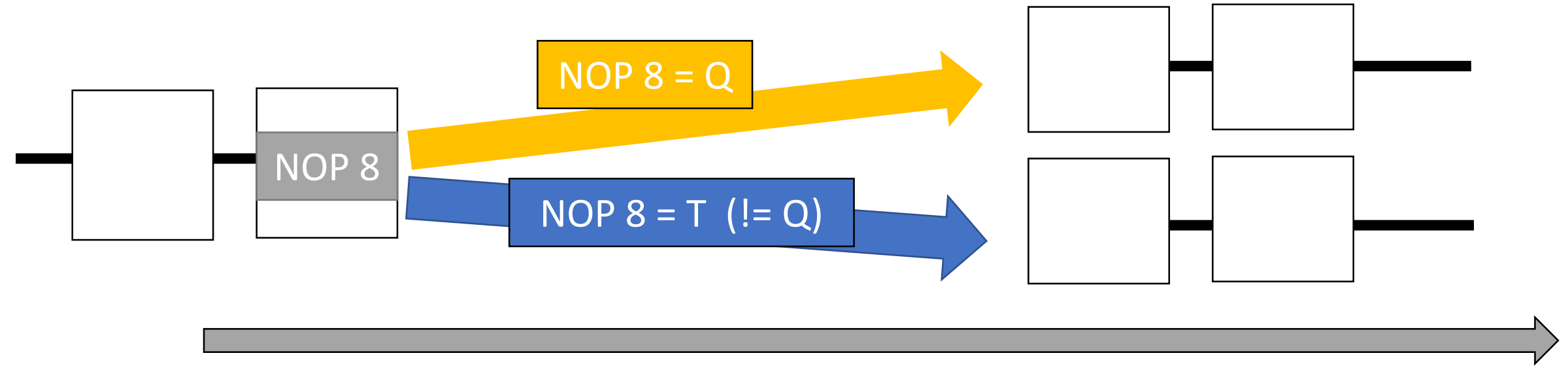
274b5686
6373f41a591f6382

Upgrading via Soft Fork

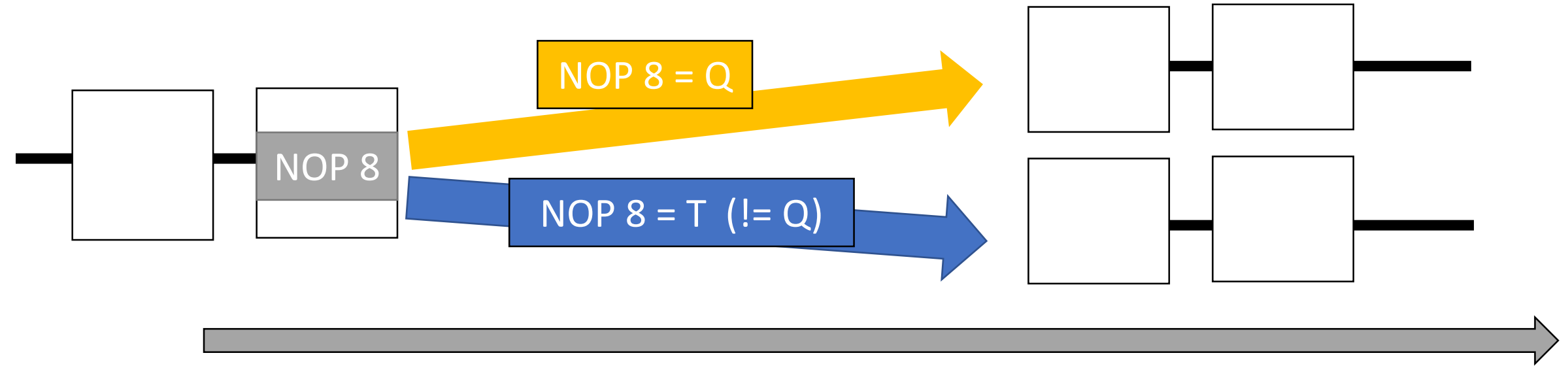
- “line” of protocols that are all compatible with each other



Two Incompatible SFs at once = HF



Two Incompatible SFs at once = HF



Begins:
“explicitly ignorable” state.

Ends: “common new” state.
(Social consensus?)

Two Incompatible SFs at once = HF

Both of these phases preceded by some
“authoritative” meta-consensus event.

“Soft” fork needs a “Hard” Setup



Begins:
“ignorable state”.



Ends: “new state”.
(Social consensus?)

Examples of “Hard Setups”

- Unused OP Codes
- Transaction Version Numbers that are Higher-than-Current
- Block Version Numbers that are “.



Added by Satoshi



Redefined by:
Satoshi / Core Developers

The Problem: Soft Fork Infinite Regress (?)

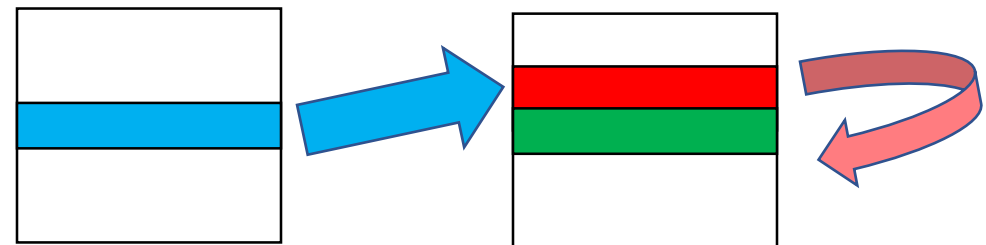
1. “What’s up for grabs?”
ie, what is in the “ignorable set”.

- OP Codes
- Txn/Block Versions
- Witnesses (SegWit)
- Legacy Bitcoin Script (P2SH)
- Everything? (The Evil Fork)
- Nothing? (Mircea Popescu crowd)

```
BIP: 66  
Layer: Consensus (soft fork)  
Title: Strict DER signatures
```

```
Thursday, 10 December, Year 7 d.Tr. | Author: Mircea Popescu  
-----BEGIN PGP SIGNED MESSAGE-----  
H: Belgium will receive payment of 1 (one) Bitcoin to any valid* Bitcoin  
   address of his specification.  
T: ===  
W: * Valid Bitcoin addresses start with a "1".  
-----BEGIN PGP SIGNATURE-----  
-----
```

2. Is the replacement acceptable?
 - Due to loudness, the replacement is semi-mandatory.
 - Extension Blocks – famous example.



“Loudness”

Original Question: Consensus About What?

More arbitrary than we care to admit:

1. Can't stay at slot 1. ("the loud payments")

2. Accurate movement
from slot to slot
is based on "authoritative" criteria.



3. Rules of movement
(meta-consensus)
are themselves disputed.

• Bitcoin 0.5.0

• Bitcoin 0.6.0

• Bitcoin 0.7.0

**Compatibility – Regresses
to the consensus problem
we originally wanted to
solve.**

Original Question: Consensus About What?

What did these two halves of the presentation have to do with each other?

Sidechains!

No  events, and no loudness.

Ironically, there is no loudness *because* “theft” is possible.

Explicit, fixed definitions fo:

- What is “ignore-able” (ie what is “up for grabs”)
- What it can be changed to (defined in a given sidechain BIP).

Conclusions

1. Sidechains **are** a layer-2.
2. Sidechains use the same security assumptions (although, different security model).
3. In fact, the *lack* of sidechains is a much bigger threat to mainchain miners.
4. Soft fork has “zones” (of “ignorable” and “defined”), the boundary and range of these zones is not clearly defined, which leads to conflict. “Bitcoin” does not have a fixed definition.

Advice

1. Remember user-sovereignty, resist sidechain FUD.
2. Check out the project at [**drivechain.info**](https://drivechain.info) , specifically the diffs.