Drivechain – Overview and Misconceptions

Paul Sztorc

TAB Conf – Atlanta, GA

Jan 27, 2018 – v1.0

Feb 4th, 2018 – v2.0

Jorge Timón @timoncc · 4h

Because people lacking time to review an idea they don't consider good is unthinkable, right? I haven't fully read it but I think I have a general understanding of drivechains. Perhaps you can confirm I'm not wrong answering a few questions.

1 3

Jorge Timón @timoncc · 4h

Drivechains require all miners to validate the sidechain to be sure you won't produce a bitcoin invalid block, is that correct?

1 1

//m@-c
@mecampbellsoup

Follow

Replying to @timoncc @Truthcoin and 15 others

Holy crap has anyone read about drivechains in this discussion?

8:23 AM - 4 Feb 2018

1 Retweet **4** Likes

2 1 4

Mr.Hodl @MrHodl · 4h

Replying to @mecampbellsoup @Truthcoin and 15 others

I haven't because DC don't interest me in anyway.

1

Mr.Hodl @MrHodl · 4h

Replying to @mecampbellsoup @Truthcoin and 15 others

I haven't because DC don't interest me in anyway.

1

//m@-c @mecampbellsoup · 4h

OK but why are you then liking tweets, etc. from others criticizing it without having researched the proposal? Obvious cult behavior.

1 1

Mr.Hodl @MrHodl · 4h

Because i'm not a fan of any changes that gives miners more power.

1 2

Tweet unavailable

Mr.Hodl @MrHodl · 4h

Replying to @MashuriBC @Truthcoin and 16 others

Not wanting miners to have more power makes me look ignorant? Right on.

2 1

//m@-c @mecampbellsoup · 4h

The claim that it gives them more power than they have today is untrue.

1

Mr.Hodl @MrHodl · 4h

If only miners validate sidechains, yes it's true.

1 1

Jorge Timón @timoncc · 4h
Because people lacking time to review an idea they don't consider good is unthinkable, right? I haven't fully read it but I think I have a general understanding of drivechains. Perhaps you can confirm I'm not wrong answering a few questions.

1

Jorge Timón @ti
Drivechains require all miners to validate the sidechain to be sure you won't produce a bitcoin invalid block, is that correct?

1 1

//m@-c
@mecampbellsoup
Follow

Replying to @
Holy cr
in this
8:23 AM - 4 F

1 Retweet 4 Likes

2 1

Mr.Hodl @
Replying to
I haven't because DC don't interest me in anyway.

1

"Drivechain gives miners more power"

"Optionality" Criterion

"DC allows users to choose to make a certain gamble: the **risk** is that I [Paul Sztorc] am correct about a given miner-strategy being objectively the most profitable, the reward is unlimited technical flexibility without the need to bother everyone else (with a hard fork)"

"Letting users gamble that a mining-policy is objectively the most profitable" -- Indistinguishable from the Lightning Network

Mr.Hodl @MrHodl · 4h
Replying to @mecampbellsoup @Truthcoin and 15 others
I haven't because DC don't interest me in anyway.

1

//m@-c @mecampbellsoup · 4h
OK but why are you then liking tweets, etc. from others criticizing it without having researched the proposal? Obvious cult behavior.

1 1

Mr.Hodl @MrHodl · 4h
Because i'm not a fan of any changes that gives miners more power.

2

C @Truthcoin and 16 others
have more power makes me look ignorant? Right on.

2 1

//m@-c @mecampbellsoup · 4h
The claim that it gives them more power than they have today is untrue.

1

Mr.Hodl @MrHodl · 4h
If only miners validate sidechains, yes it's true.

1 1

The Problem – People are Different

On Wednesday 14 June 2017 10:20:33 PM
Sergio Lerner via Bitcoin-segwit2x
wrote:

> There are two group of people which have two different visions for Bitcoin.
>
> None of these visions is "wrong".
>
> One group values more things like decentralization, lack of government,
> censorship resistance, anonymity. This group thinks that Bitcoin will
> transform our world in 20-30 years. To reach this goal, it's of utter
> importance to stick to those values. There is no rush.
>
> The other group values more things like reaching one billion users in the
> next 5 years, or serving real unbanked users today, even if that requires a
> political agreement now.
>
> Both visions have their merits. But they are incompatible.

Drivechain?

On Wednesday 14 June 2017 10:2
Sergio Lerner via Bitcoin-segw
wrote:
> There are two group of people which have two different vi
>
> None of these visions is "wrong".
>
> One group values more things like decentralization, lack
> censorship resistance, anonymity. This group thinks that
> transform our world in 20-30 years. To reach this goal, i
> importance to stick to those values. There is no rush.
>
> The other group values more things like reaching one bill
> next 5 years, or serving real unbanked users today, even
> political agreement now.
>
> Both visions have their merits. But they are incompatible

Luke Dashjr luke at dashjr.org
Fri Jun 16 04:32:51 UTC 2017

- Previous message: [bitcoin-discuss] Scaling Sidechain -- spec / blocksize limit (h
- **Messages sorted by:** [date] [thread] [subject] [author]

(I think this thread might be off-topic for Segwit2x, so I'm redirecting to the bitcoin-discuss@ mailing list.)

IMO, these two visions are *not* fundamentally incompatible. (For the purposes of this email, I am going to refer to the two groups as "decentralisation-first" and "adoption-first", respectively.)

Paul Sztorc's drivechains concept can potentially deliver miner-controlled, much larger blocks in the near future. This comes at the expense of decentralisation, of course, but as a drivechain, this loss does not directly affect the main chain, which can continue to develop according to the goals of the decentralisation-first group. There is a reduction in security of the drivechain since miners effectively make all the final decisions for it, but the adoption-first group tends to embrace and desire this miner-driven model anyway.

So by using a drivechain, it is in fact possible to achieve two blockchains achieving the goals of each group, and both remaining part of the same Bitcoin network and using the same bitcoins.

Luke

Drivechain?

Stickied by theymos -- top of /r/bitcoin for two weeks

r/bitcoin

this post was submitted on 16 Jun 2017
570 points (91% upvoted)
shortlink: https://redd.it/6hpkqd

570

How to get both decentralisation and the bigblocker vision on the same Bitcoin netwo

submitted 7 months ago by luke-jr

284 comments share save hide give gold report crosspost

Luke
Fri Jun 16 04:32:51 UTC 2017

spec / blocksize limit (h
r]

I'm redirecting to

> importance to stick to those values. There is no rush.
>
> The other group values more things like reaching one bill
> next 5 years, or serving real unbanked users today, even
> political agreement now.
>
> Both visions have their merits. But they are incompatible

IMO, these two visions are *not* fundamentally incompatible. (For the purposes of this email, I am going to refe
first" and "adoption-first", resp

Paul Sztorc's drivechains concept

Oct 3, 2016 at 16:59 UTC

Blockstream

Adam Back @adam3us · 29 Oct 2017

Replying to @adam3us @JihanWu and 2 others

as I've explained to yourself & Micree for a while now, best chance is lightning, and **drivechain**. why not contribute & help scale Bitcoin?

7 2 25

in fact possible to achieve
achieving the goals of each group, and both remaining part of the same Bitcoin network and using the same bitcoins.

Luke

Agenda

1. Review: What are Sidechains?
2. ‘Drivechain’ Specifically
   a) Puzzle Pieces / Existing Ingredients
   b) Achieving “Opt-In”
   c) Fusion of Ideas –> Slow, Transparent Withdrawals
3. Security Model of Drivechain – often misunderstood
4. Blind Merged Mining
5. Helpful Comparisons

What are sidechains?

Drivechain

Drivechain allows multiple blockchains to all agree to share the same 21,000,000 Bitcoins. These networks are otherwise autonomous.

From Project Site

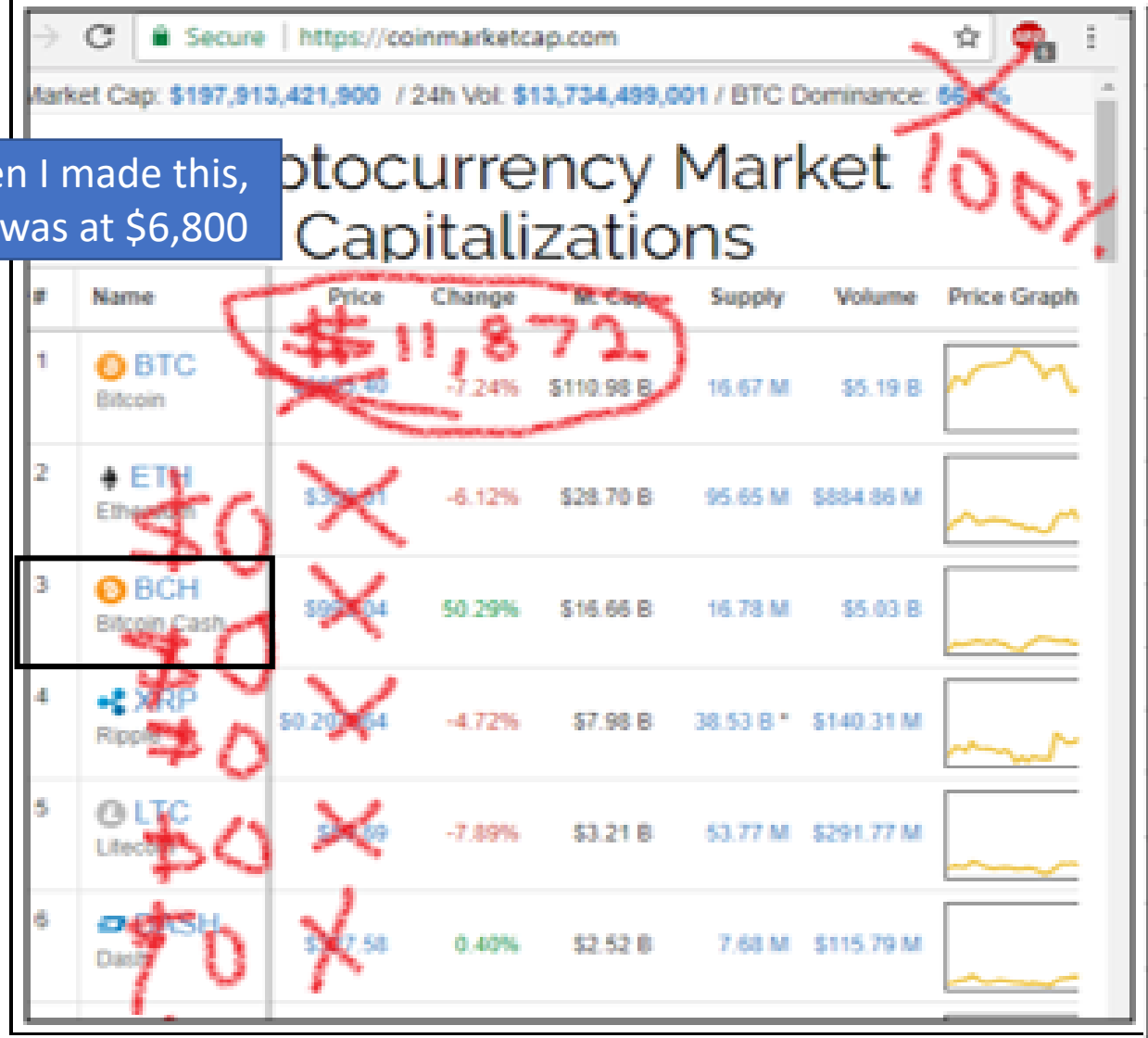
www.drivechain.info

- An "**alt-chain**" is a blockchain with "alt" rules and abilities. (Different cost/benefit tradeoff.) :)
  - "**alt-coin**" = alt-chain + new *monetary network*.
  - "**sidechain**" = alt-chain + inherits *monetary network*.
  - (Note that *mone. networks* are *inherently adversarial.*) :(

What's the point?

Popularity → d(location), not d(price)

When I made this, BTC was at $6,800



Coin Locations

	BTC	% Total
Bitcoin Core	10,250,983	61.5%
Bit-Ethereum	551,675	3.3%
Bit-Monero	674,370	4.0%
Bitcoin Unlimited	1,650,202	9.9%
Bitcoin Cash	1,497,040	9.0%
Bit-Mimble	1,984,302	11.9%
...	42,897	0.3%
Bit-DAO	16,501	0.1%
Bit-TEZOR	740	0.0%
Bit-StupidProject	1,239	0.0%
Bit-Whatever	51	0.0%
Subtotal	16,670,000	100.0%
Not-Yet-Mined	*4,330,000*	
Grand Total	21,000,000	

What's the point?

- Crush the Alts
  - Value – Metcalfe's Law
  - Blockspace & Security – Alt Tx Fees to Our Miners
  - Existential Threat
- Scalability Contention
  - True cause: **people are different** (vs blockchain 100% consensus)!
  - Lightning network <u>*does not solve scalability contention*</u>
  - "miles per gallon" (scalability) vs. "fuel tank size [gallons]" (decentralization)
  - "Scalability" debate *isn't about scalability*. It is about <u>***decentralization***</u> -- how much a node should cost to run.

Scalingbitcoin

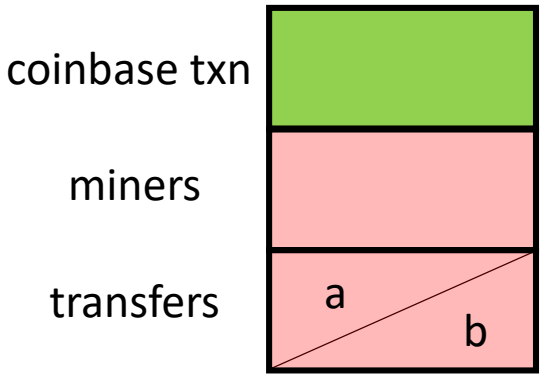
Roger / Luke

Part 2 – Drivechain

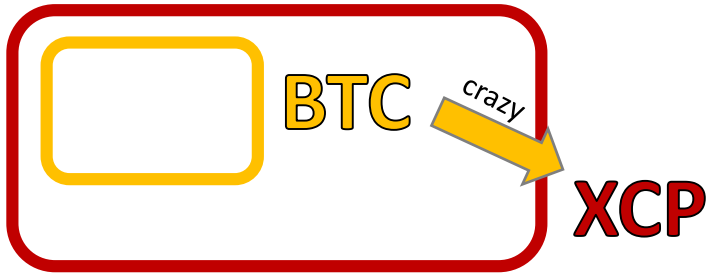
How do we make this wonderous technology?

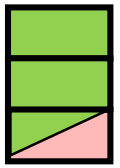
Existing Ingredients -- get us Mostly There

1. **Altcoins Themselves** – LTC, Eth – would *already* be sidechains if not for…
   i. …they print their own money.
   ii. …they reliably have their own miners/consensus.
   iii. …they lack *accounting rules* for interchain transfers.
      a. Mainchain balance down by 1 → Sidechain balance up by 1
      b. Sidechain balance down by 1 → Mainchain balance up by 1

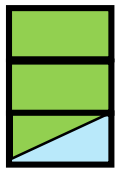


2. **Embedded Consensus** – Counterparty, Colored Coins
   1. Inherits Consensus ("Merged" Mining)
   2. Asymmetric Protocol
      "Child Watches Parent" – "deposits" tightly controlled





3. Instant Atomic **Cross-Chain Swaps**
   1. Zero-trust, simple, and *fast*… (1 block w/o LN, immediate w/ LN)
   2. …but not 'pegged' (not *forced* to be at desired 1:1 fixed rate).



(You deposit 10 Core-BTC into RSK, making it 10 Ethereum-BTC. But will anyone willingly give you 10 Core-BTC for Eth-BTC?)
(We want all the Altcoin-related price risk to be hedged away.)

Part 2b – Achieving "Opt-In"

Before I talk about the ***pegged main-to-side xfers***, I need to talk about some other things.

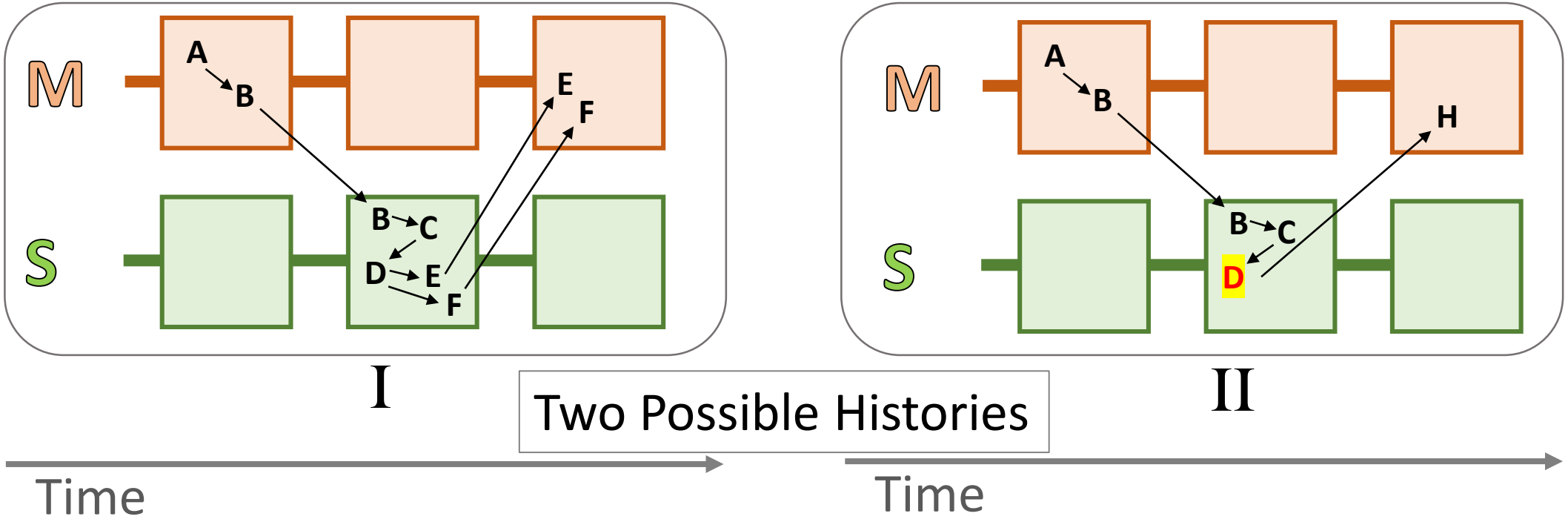
Warning: Advanced Blockchain Theory Ahead!

8 difficult slides

1/8

The Sidechain Must be Optional

- By definition, the **sidechain must be optional**.
  - Mainchain must process withdrawals "blind" to what is going on in the sidechain.
  - Otherwise, it would be a de facto hard fork (which is exactly what we are trying to avoid in the first place). **Can't be "opt in" unless you are "out" by default.**
- But, then, an *invalid withdrawal* must be treated **exactly the same** as a valid one! There is no basis for discriminating between them.



2/8

The Sidechain Must be Optional

- By definition, the sidechain must be optional.
  - Mainchain must process withdrawals "blind" to what is going on in the sidechain.
  - Otherwise, it would be a de facto hard fork (which is exactly what we are trying to avoid in the first place). **Can't be "opt in" unless you are "out" by default.**
- But, then, an invalid withdrawal must be treated **exactly the same** as a valid one! There i[illegible]hem.

Side-to-main xfers:

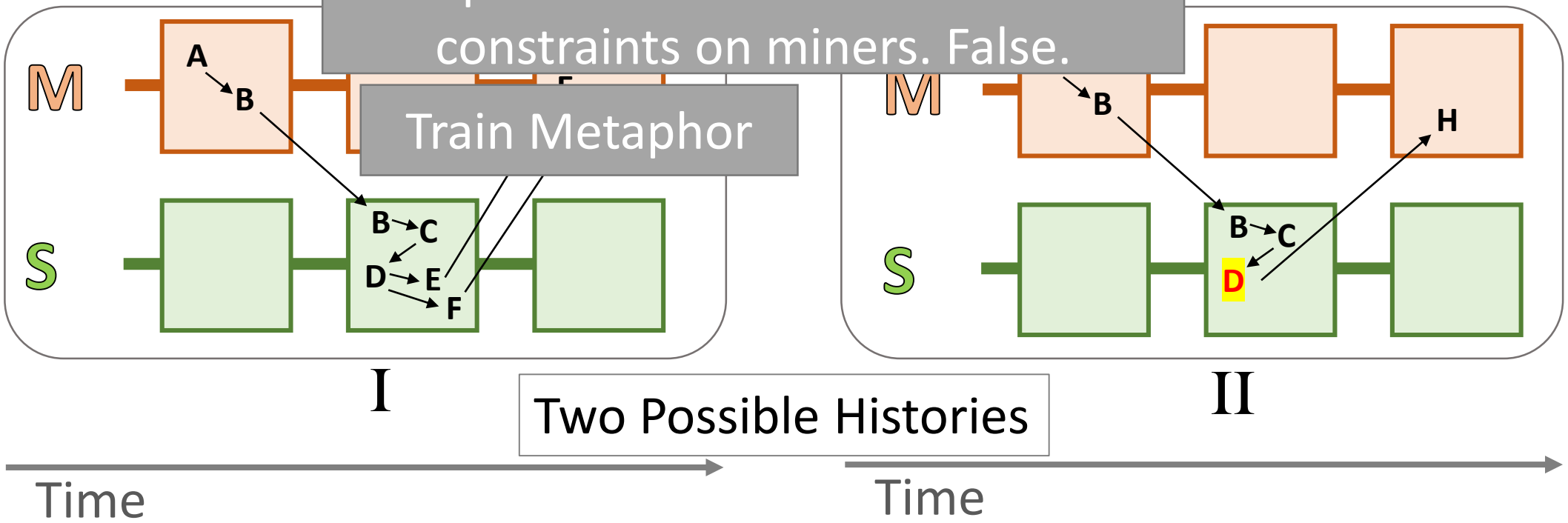
1. … ***must*** be free to go ***anywhere***.
2. … ***cannot*** be constrained by ***node*** validation.
3. (These are pros, not cons!)

But, if txn is unrestrained, *anyone* can immediately steal its BTC….

Fortunately, we ***can*** constrain S2M by ***SPV*** validation – ie , if scarce (non-reusable) proof of work has been done on S2Ms.

Slepak Error – No main:fullnode constraints on miners. False.

Train Metaphor



Two Possible Histories

3/8

The Si

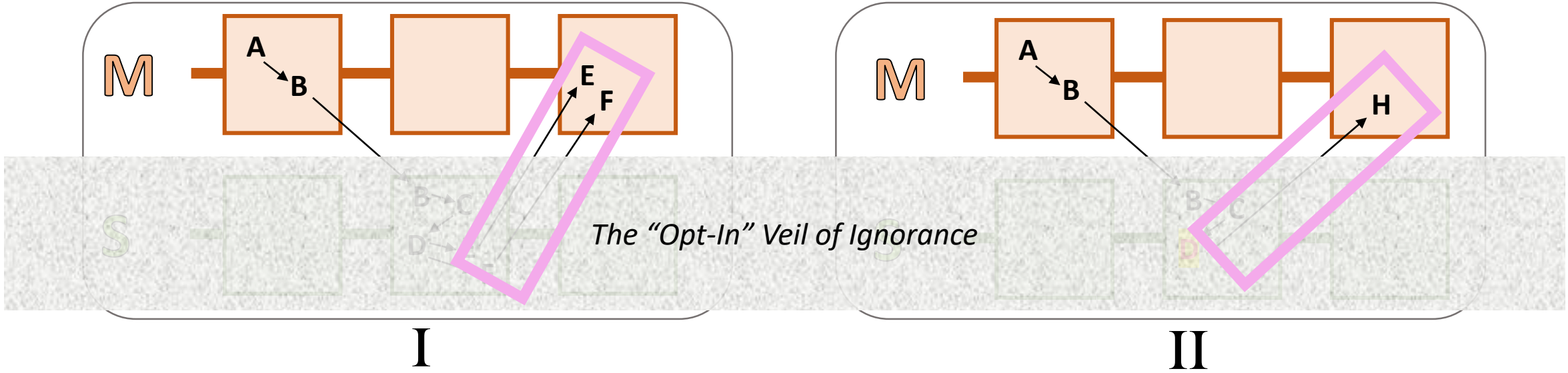
Side-to-main xfers:

1. … ***must*** be free to go ***anywhere***.
2. … ***cannot*** be constrained by ***node*** validation.
3. (these are pros, not cons)

- By defini

Ignorance Mandate

- ***If you want to know*** which withdrawals are side:valid, then run the sidechain node.
- ALL this tech is for the people who *don't* want to run the sidechain node…
  …in other words, ***the people who don't want to know***.



One of these is SC-theft. But which one?

4/8

Users Affect Miners Affect Users (UsAMAUs)

Some users → All Miners [intransigent minority; uasf]

All Miners → All users [“Am I getting paid?”; chain status]

If miners are persuaded to follow different [but compatible] rules, then you’re stuck with them as well!

e sidechain node.

- AL this tech is for the people who *don't* want to run the sidechain node…

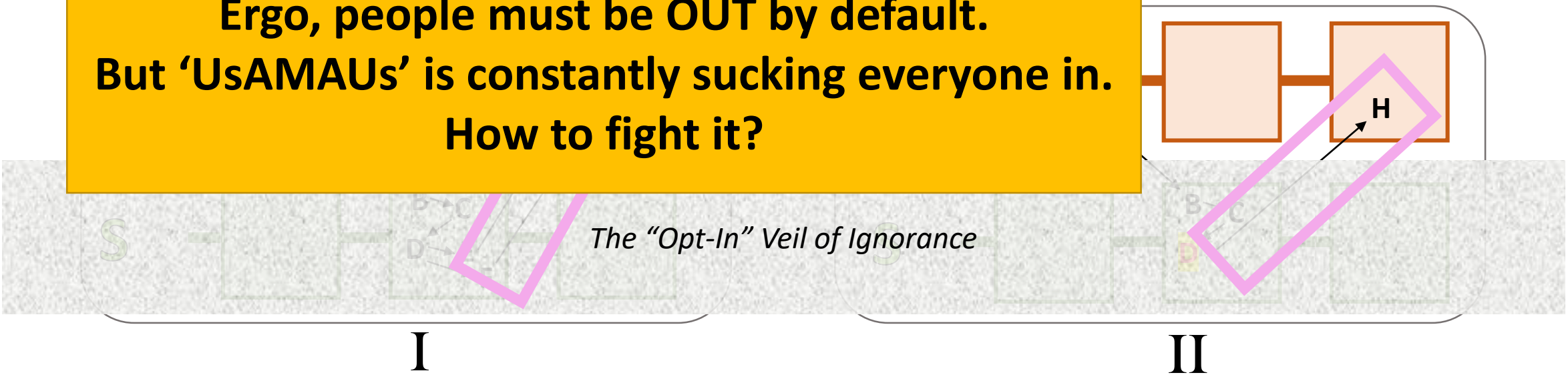
…i

We want “opt in”.

Ergo, people must be OUT by default.

But ‘UsAMAUs’ is constantly sucking everyone in.

How to fight it?



One of these is SC-theft. But which one?

5/8

The Si

Side-to-main xfers:

1. ... must be free to go anywhere;

- By

Ignc

- *If y*
- AL

...ir

Mandatory

several optional "smart contracts" have already been forked into BTC (RSK federation, XCP, Mt Gox website).

Peter Todd
@peterktodd

Following

Replying to @bohrexciton @GMikeska and 2 others

A sidechain that has been soft-forked in is no longer a sidechain, it's a blocksize increase, just like segwit.

8:37 AM - 6 Jan 2018

1 Retweet **11** Likes

Mandatory sidechain = today called "extension block"

Preceding tweet

Peter Todd @peterktodd · Jan 6

The problem with mined sidechains is that the segwit "anyone-can-spend" issue is a reality, not FUD, and miners can steal sidechain funds; the reason why segwit doesn't have that problem is because full nodes prevent the theft, but sidechains have only miner-trusting SPV.

One of these s SC-theft. ut which one?

Problem with extension blocks, is ironically, **miners can't steal from them**, ie that ext-blocks ***force people to know***.

Mutually-Exclusive Criteria

6/8

Peter Todd
@peterktodd

Following

Replying to @bohrexciton @GMikeska and 2 others

mandatory

A sidechain that has been soft-forked in is no longer a sidechain, it's a blocksize increase, just like segwit.

8:37 AM - 6 Jan 2018

Sidechain must be optional

1 Retweet 11 Likes

PT's point is even true for zk-snarks / CoinWitness – those would be a non-optional 'evil fork' (soft-hardfork)…albeit a hopefully irrelevant one.

7/8

“Stealing” Bitcoin

Marcel Jamin ⚡ @marceljamin · 28 Dec 2017
> DRIVECHAIN'S SECURITY
> This model allows a 51% miner coalition to actually steal Bitcoins.

/thread

1

Paul Sztorc @Truthcoin · 28 Dec 2017
A very dishonest summary

2

Marcel Jamin ⚡ @marceljamin · 28 Dec 2017

1

Marcel Jamin ⚡
@marceljamin
Follow

Replying to @Truthcoin @viaj3ro and 3 others

Explanation of likeliness, not possibility.

I'm not trying to shit on drivechains. I'm totally unqualified to make any meaningful assessment here. But AFAICT that the quoted fact is a characteristic not shared by SW or LN

Greg Slepak @taoeffect@mastodon.social @taoeffect · 16 Jun 2017
What's preventing them from withdrawing entire balance on the Drivechain and claiming it as theirs?

4

Luke Dashjr @LukeDashjr · 16 Jun 2017
Nothing stops that with the bigblocker "miners in control" model. At least with drivechains, however, withdrawl is slow, so can be blocked.

1 1

Greg Slepak @taoeffect@mastodon.social @taoeffect · 16 Jun 2017
How? By who?

1 1

Luke Dashjr @LukeDashjr · 16 Jun 2017
Well, since this can only occur when a supermajority of miners are participating in the attack, blocking it would be a UASF.

1 3

Greg Slepak @taoeffect@mastodon.social @taoeffect · 16 Jun 2017
OK, Drivechains are officially dumb.

1 1 1

Greg Slepak @taoeffect@mastodon.social
@taoeffect
Follow

Replying to @taoeffect @LukeDashjr

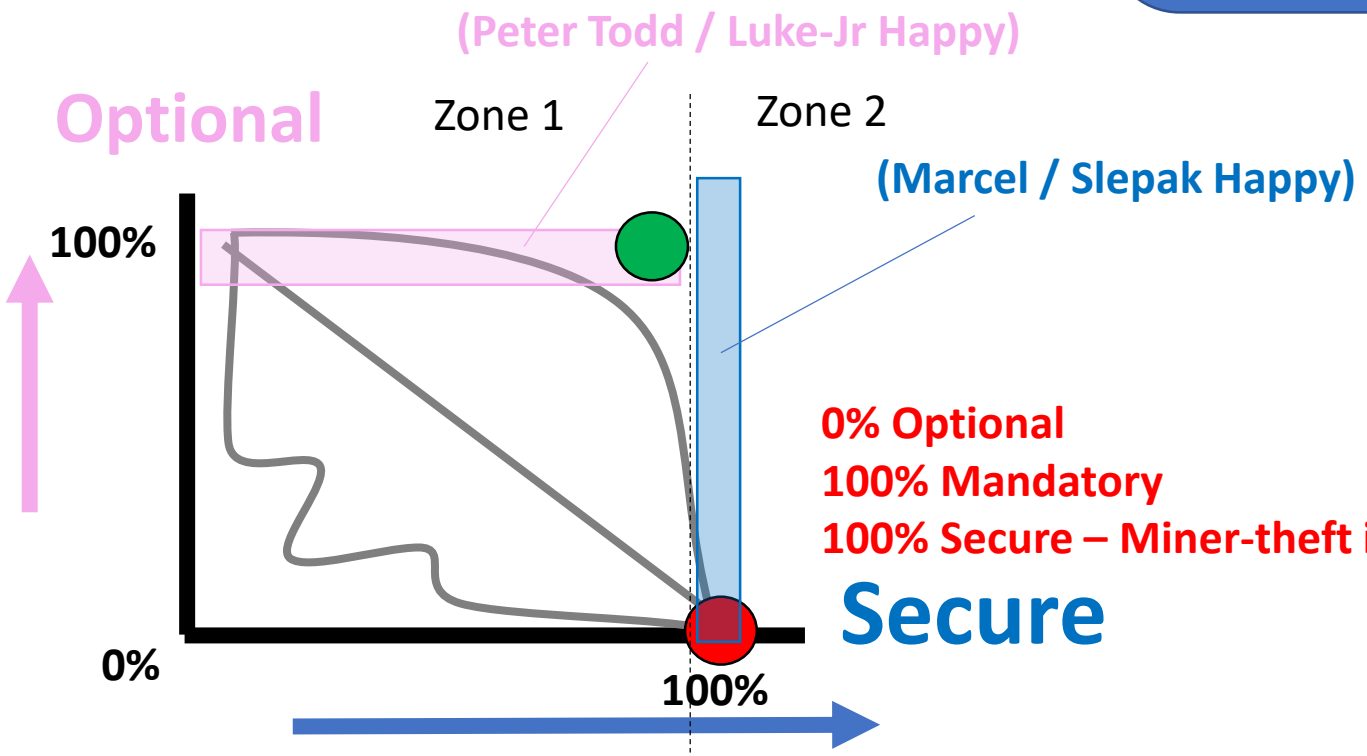
Drivechain security model is a complete regression back to banking.

8/8

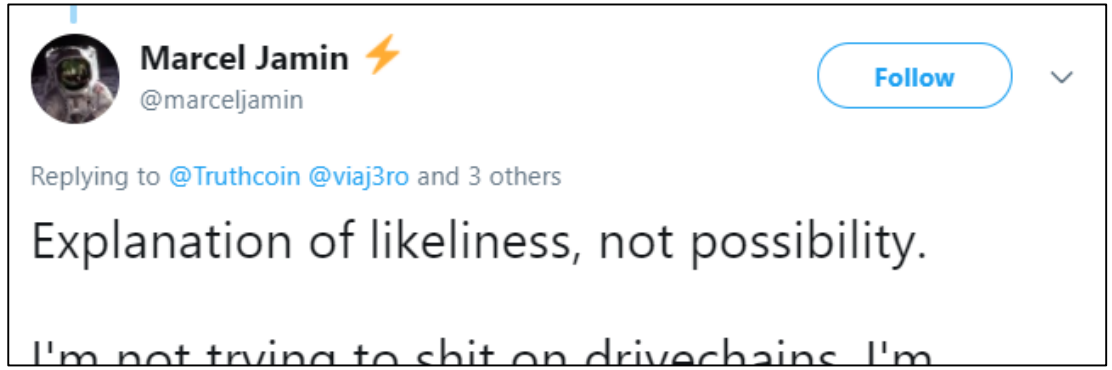
Mutually-Exclusive Criteria

Peter Todd / Luke Dashjr: ***miner-theft should be possible*** . Main:users must be able to ignore sidechain. Main:users must believe that ***main:miners will not change the main:chain*** as a result of what happens on a sidechain.

Marcel / Slepak: want miner-theft to be ***impossible***.



0% Optional
100% Mandatory
100% Secure – Miner-theft is "Impossible"



Mutually-Exclusive Criteria

[bitcoin-dev] Generalized sharding protocol for decentralized scaling without Miners owning our BTC

2017-10-10 11:09 GMT-03:00 Tao Effect via bitcoin-dev <bitcoin-dev at lists.linuxfoundation.org>:

> *When you transfer them back, you get newly minted coins, equivalent to the*
> *amount you "burned" on the chain you're transferring from – as stated in*
> *the OP.*
>

If you have to change Bitcoin to recognize a transfer from the sidechain back into Bitcoin, you kill the purpose of the sidechain. You could as well just change the Bitcoin to implement whatever desirable features the sidechain would have. The whole idea of sidechains is to keep Bicoin unchangend, and allow for the voluntary transfer of tokens out of Bitcoin to the sidechain of your choosing.

--
Lucas Clemente Vella
lvella at gmail.com

0%

100%

Revisited

Marcel Jamin ⚡ @marceljamin · 28 Dec 2017

> DRIVECHAIN'S SECURITY

> This model allows a 51% miner coalition to actually steal Bitcoins.

/thread

1

Revisited

Marcel Jamin ⚡ @marceljamin · 28 Dec 2017

> DRIVECHAIN'S SECURITY

> This model allows

the sidechain to be optional….

1

…thus ***protecting*** mainchain users from being kept in the dark about the status of their mainchain payments.

Revisited

Marcel Jamin ⚡ @marceljamin · 28 Dec 2017

> D ForceNet N'S SECURITY

> This model forces full nodes to validate all sidechain rules, ***preventing theft***…

/thread

…but ***forcing*** mainchain users to upgrade, as in a "hard fork", or "evil fork" or "Soft-hardfork", like extension blocks (incl SegWit).

https://bitcoinhardforkresearch.github.io

Bitcoin Hard Fork Research

This website will be updated with relevant ongoing information about Bitcoin hard fork research.

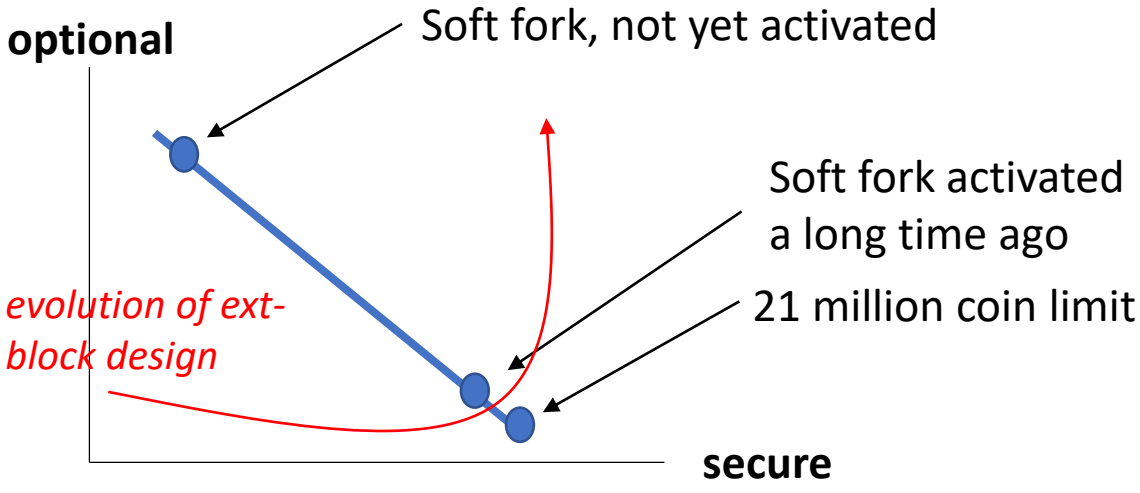
- BIP-MMHF, draft patch last updated 2016/7/17, discussion, Luke-Jr, 2016/2/7
- BIP-MSMMHHF, ML discussion, James Hilliard, 2016/2/23
- Research update by Peter Todd, 2016/8/5
- Draft BIP: Hardfork warning system - Dr Johnson Lau, 2016/12/1
- Forcenet1 experimental hard fork testnet by Dr Johnson Lau, 2016/12/4
- Forcenet2 an experimental network with a new header format by Dr Johnson Lau, 2017/1/14
- Anti-transaction replay in a hardfork by Dr Johnson Lau, 2017/1/24

Because of 'UsAMAUs', SegWit is an ext-block / "evil fork" and NOT 100% Opt-In.

ForceNet = mandatory sidechain + 51% censorship attack.

Evil Fork (Hard Fork) or *Permanent* Inferiority

Dr. B figured out *a lot* of this back in 2014



[Bitcoin-development] soft-fork block size increase (extension blocks) Re: Pro

Adam Back adam at cypherspace.org

Sat May 30 00:00:28 UTC 2015

I discussed the extension block idea on wizards a while back and it is a way to soft-fork an opt-in block-size increase. Like everything here there are pros and cons.

The interesting thing is this makes block sizes changes opt-in and gives users choice. Choice is good. Bitcoin has a one-size-fits-all blocksize at present hence the block size debate. If a bigger block-size were an opt-in choice, and some people wanted 10MB or even 100MB blocks for low value transactions I expect it would be far easier a discussion - people who think 100MB blocks are dangerously centralising, would not opt to use them (or would put only small values they can afford to lose in them). There are some security implications though, so this also is nuanced, and more on that in a bit.

1MB full node users who do not upgrade to software that understands extension blocks, could run in SPV mode with respect to 10MB blocks. Here lies the risk - this imposes a security downgrade on the 1MB non-upgraded users, and also on users who upgrade but dont have the bandwidth to validate 10MB blocks.

mandatory extension block = hard fork in practice

We could defend non-upgrade users by making receiving funds that came via the extension block opt-in also, eg an optional to use new address version and construct the extension block so that payments out of it can only go to new version addresses.

ignorable extension block = permanent second class citizens

Mandatory extension block ***requires you to know***.

Optional extension block – pretty secure, but ***one way*** – not pegged and thus not as *useful.*

Dr. B – Extension Block vs Drivechain

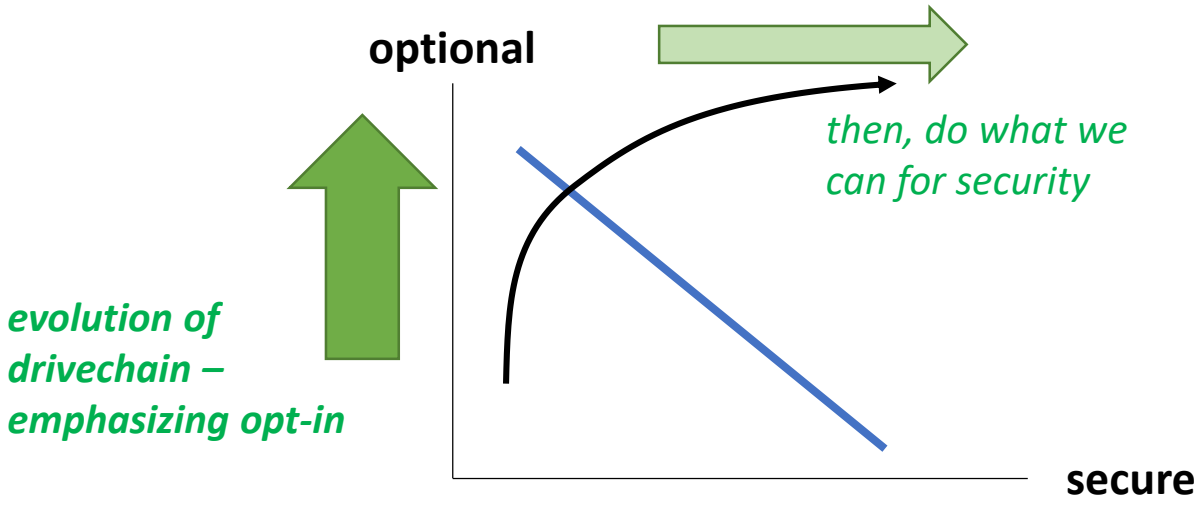
Adam Back @adam3us · 14 Nov 2017

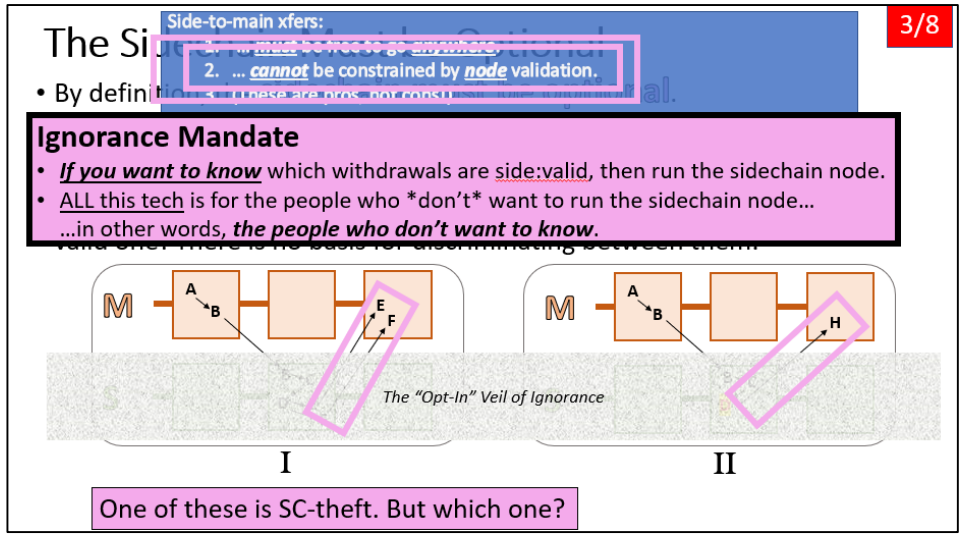
Replying to @Truthcoin @AlpacaSW

well it's not a free lunch though: ext-blocks externalise validation costs for bitcoin holders and users. I think people more prefer the **drivechain** approach, as then the code is not expanding consensus critical code, nor as directly increasing required data to validate main chain

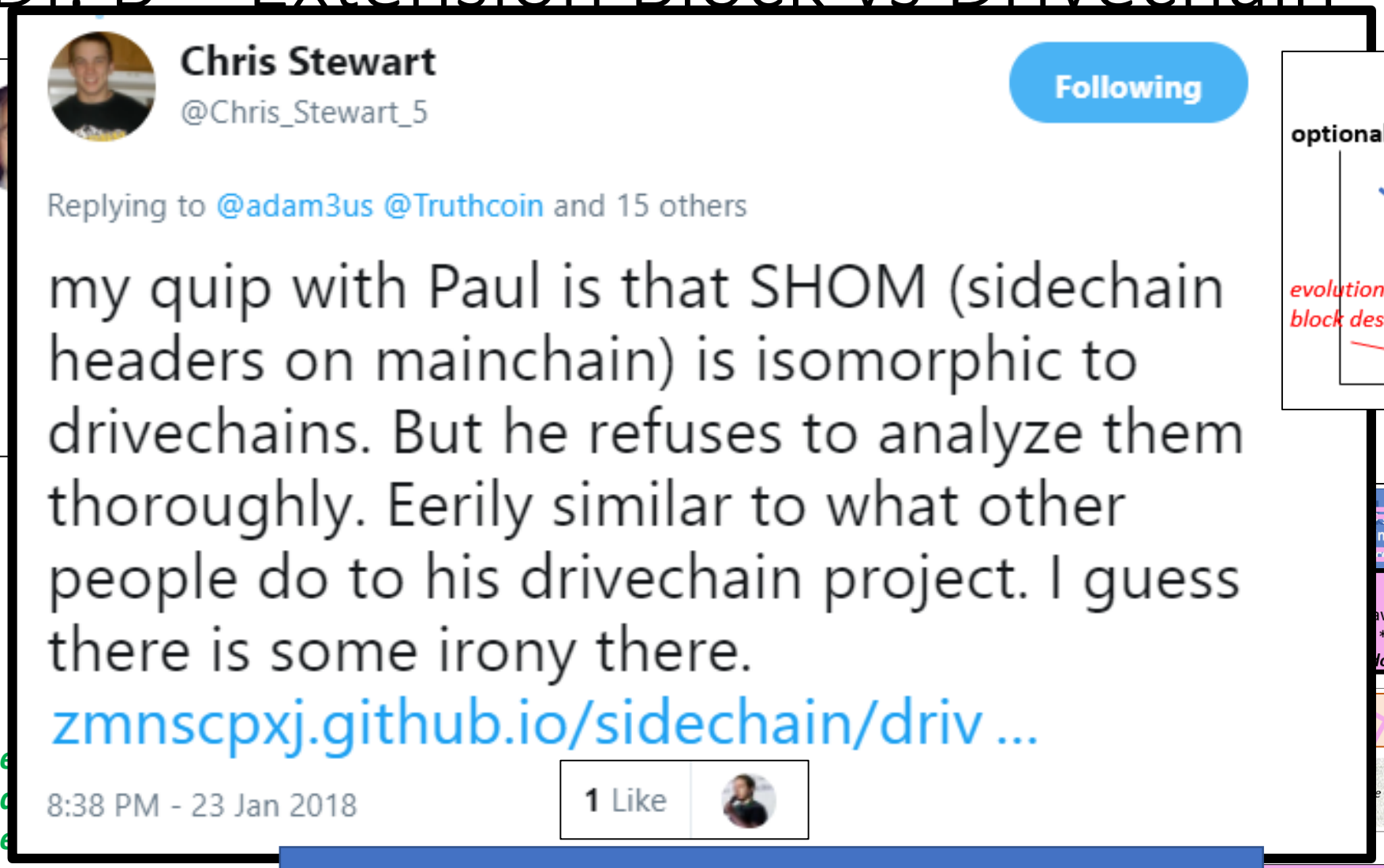
1 2

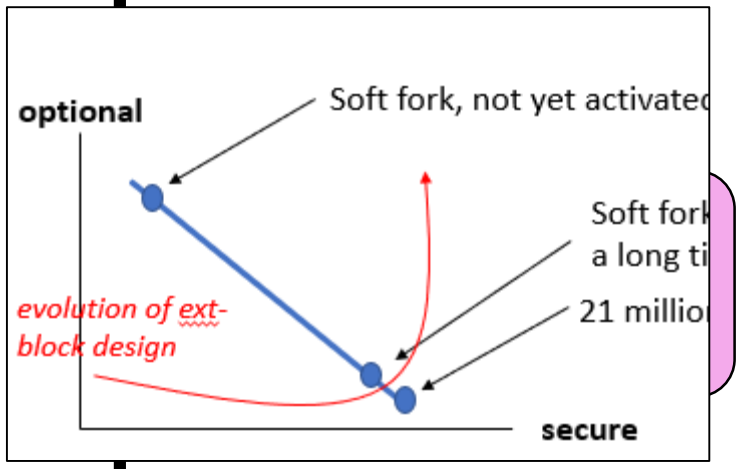
Drivechain: mandatory trivialities (for miners). Optional everything (for users).

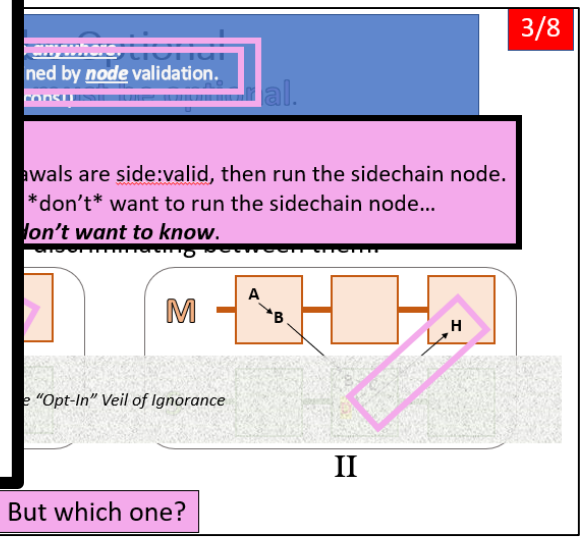




Dr. B – Extension Block vs Drivechain







Liked by Giacomo Zucco, CEO Blockchainlab.it

Misunderstood from Both Sides

Alphonse Pace
@AlpacaSW

Follow

Replying to @viaj3ro @Truthcoin and 18 others

The meaningful downside is I now have to pay attention and validate something I never cared to. Play stupid games, win stupid prizes.

10:42 AM - 4 Feb 2018

1 Like

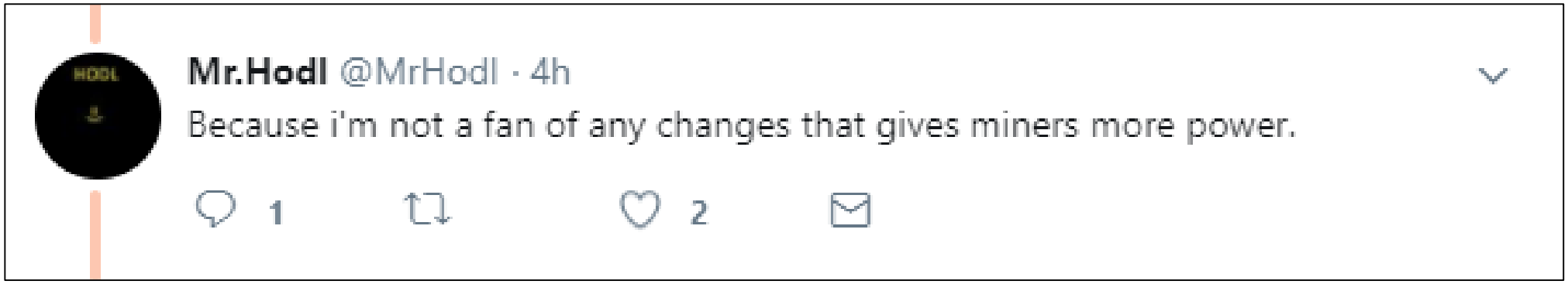
Liked by Giacomo Zucco, CEO Blockchainlab.it

1 1

Alp prefers it to be Optional

...even though it already is.

Misunderstood from Both Sides



Does he know :
* …he disagrees with Todd/ Dashjr / Alp ?
* this arg would disqualify ALL sidechain designs ?

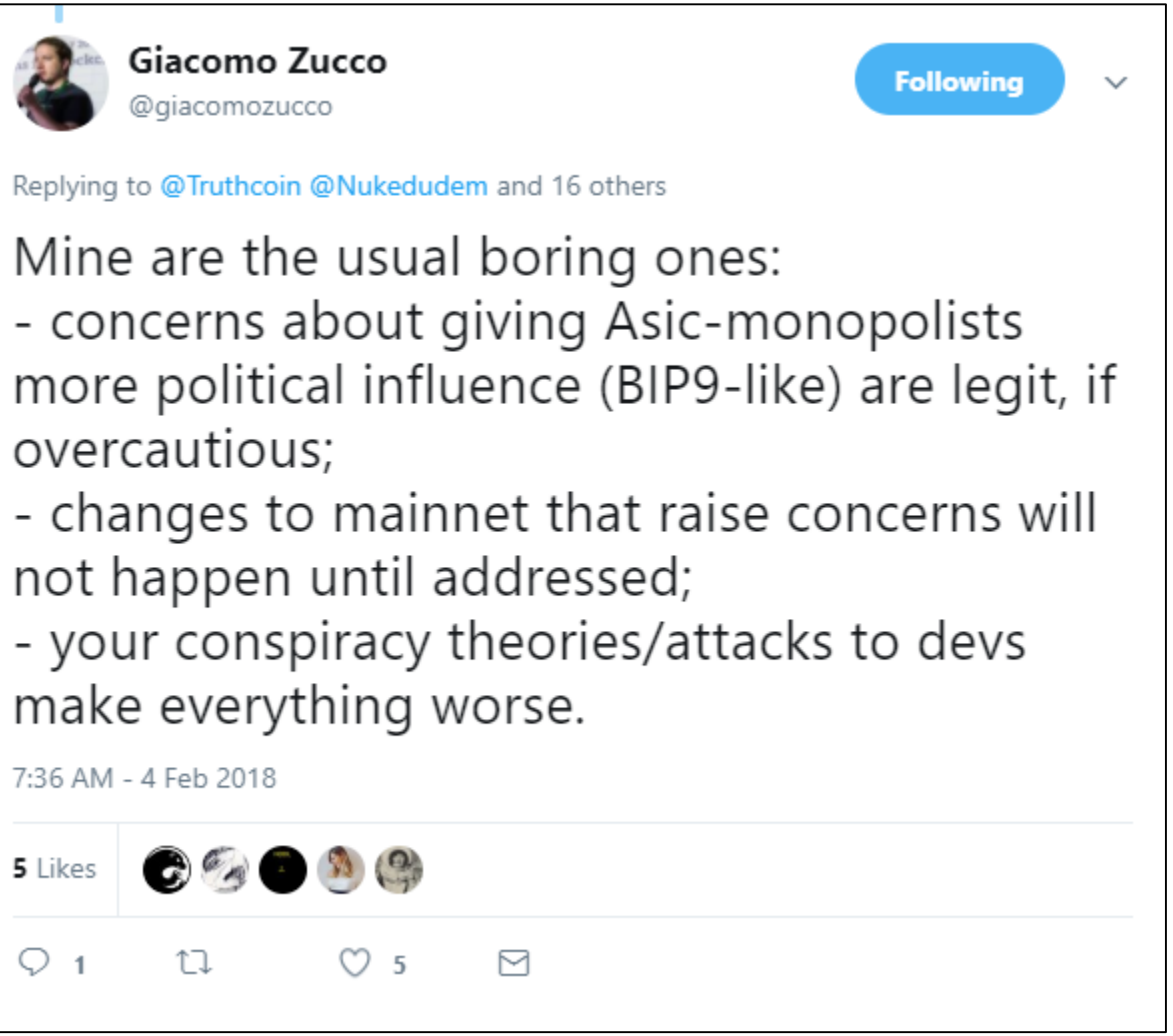
MrHodl prefers it to be Mandatory (ie, node-secured)

Misunderstood from Both Sides

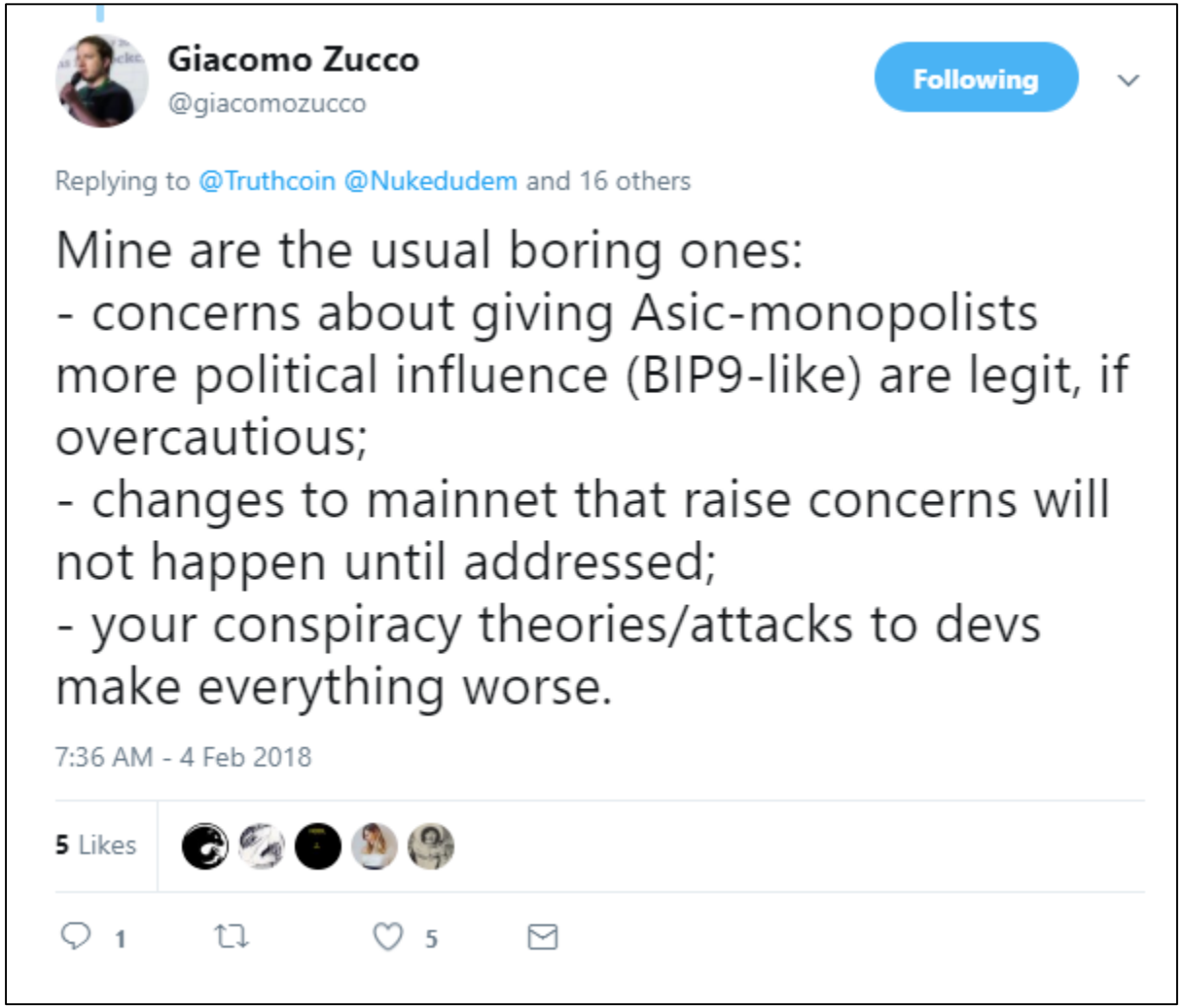
Does he know :
* …he disagrees with Todd/ Dashjr / Alp ?
* this arg would disqualify ALL sidechain designs ?

MrHodl prefers it to be Mandatory (ie, node-secured)

A Crazy UsAMUs



A Bizarre UsAMUs



Two Models

Desire for Power → **Miner's Decisions**

Profit Motive → **Miner's Decisions**

SegWit Withheld – Profit Motive?

Scaling 3 – too little too late

2016 in context – rise of Eth / Alts
Earnest confusion about ***how*** to
Profit-maximize, breakdown of Communication

Scaling 2 – Miner roundtable

A Bizarre UsAMUs

Two Models

Desire for Power → **Miner's Decisions**

Profit Motive → **Miner's Decisions**

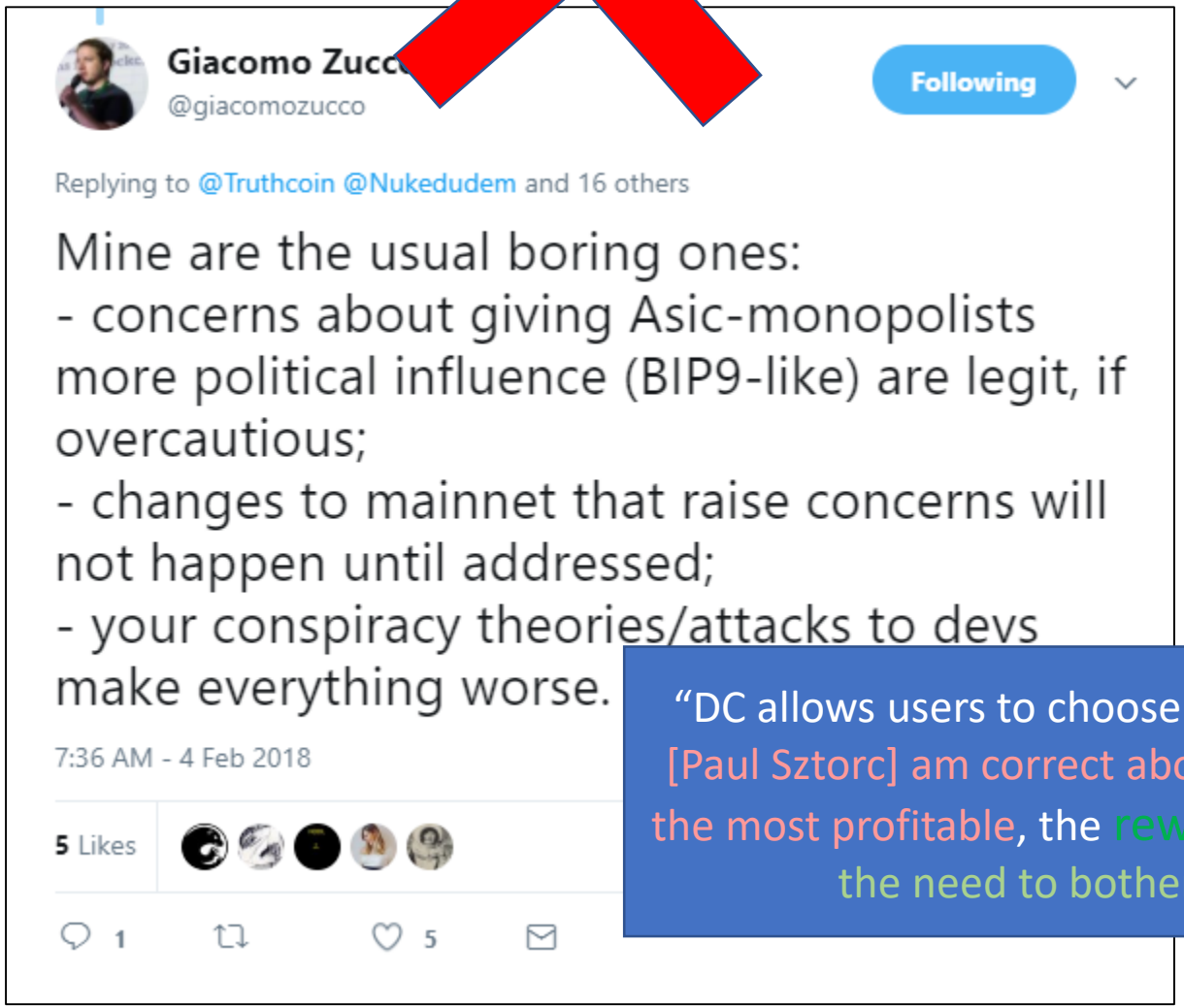
SegWit Withheld – Profit Motive?

Scaling 3 – too little too late

2016 in context – rise of Eth / Alts
Earnest confusion about ***how*** to
Profit-maximize, breakdown of Communication

Scaling 2 – Miner roundtable

A Bizarre UsAMUs



Actually not a UsAMUs

Only the speculators are affected.

Just the "but SC users might lose the gamble" arg in disguise.

"DC allows users to choose to make a certain gamble: the **risk** is that I [Paul Sztorc] am correct about a given miner-strategy being objectively the most profitable, the reward is unlimited technical flexibility without the need to bother everyone else (with a hard fork)"

tion

Fusion of Ideas…

Mainchain txn rules:

- *Already* prevent counterfeiting.
- Can *never* (by definition) enforce sidechain rules.

(Theft-notwithstanding a "peg" has achieved itself).

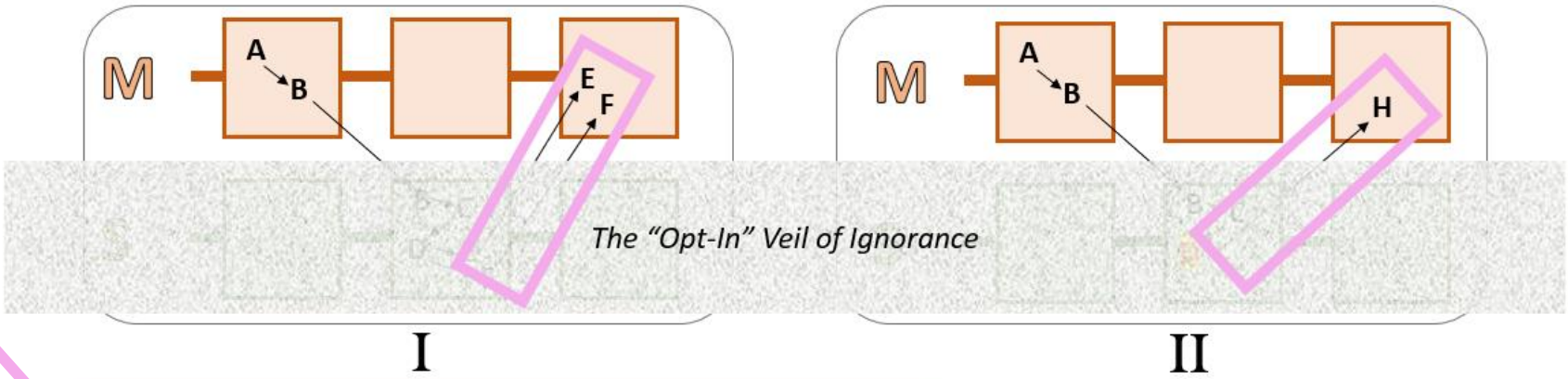
Our unsolved problem is *theft*, not "peg".

Secure | https://en.bitcoin.it/wiki/Protocol_documentation

ript) is the recipient of the funds.

In a transaction, the sum of all inputs must be equal to or greater than the sum of all outputs. If the inputs exc

the difference is considered a transaction fee, and is redeemable by whoever first includes the transaction in



One of these is SC-theft. But which one?

ACCS – no theft, easy to use, and ***fast***…

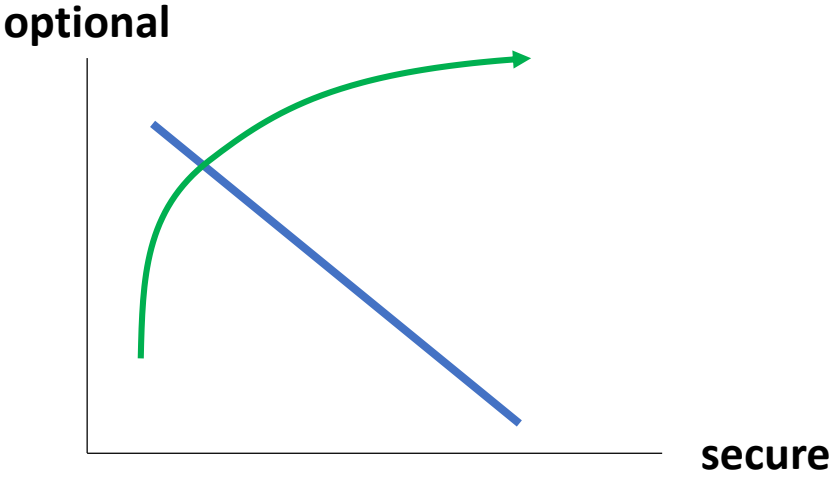
Child Watches Parent – "deposits" tightly controlled

XCP

3. Instant Atomic **Cross-Chain Swaps**
   1. Zero-trust, simple, and *fast*… (1 block w/o LN, immediate w/ LN)
   2. …but not 'pegged' (not *forced* to be at desired 1:1 fixed rate).

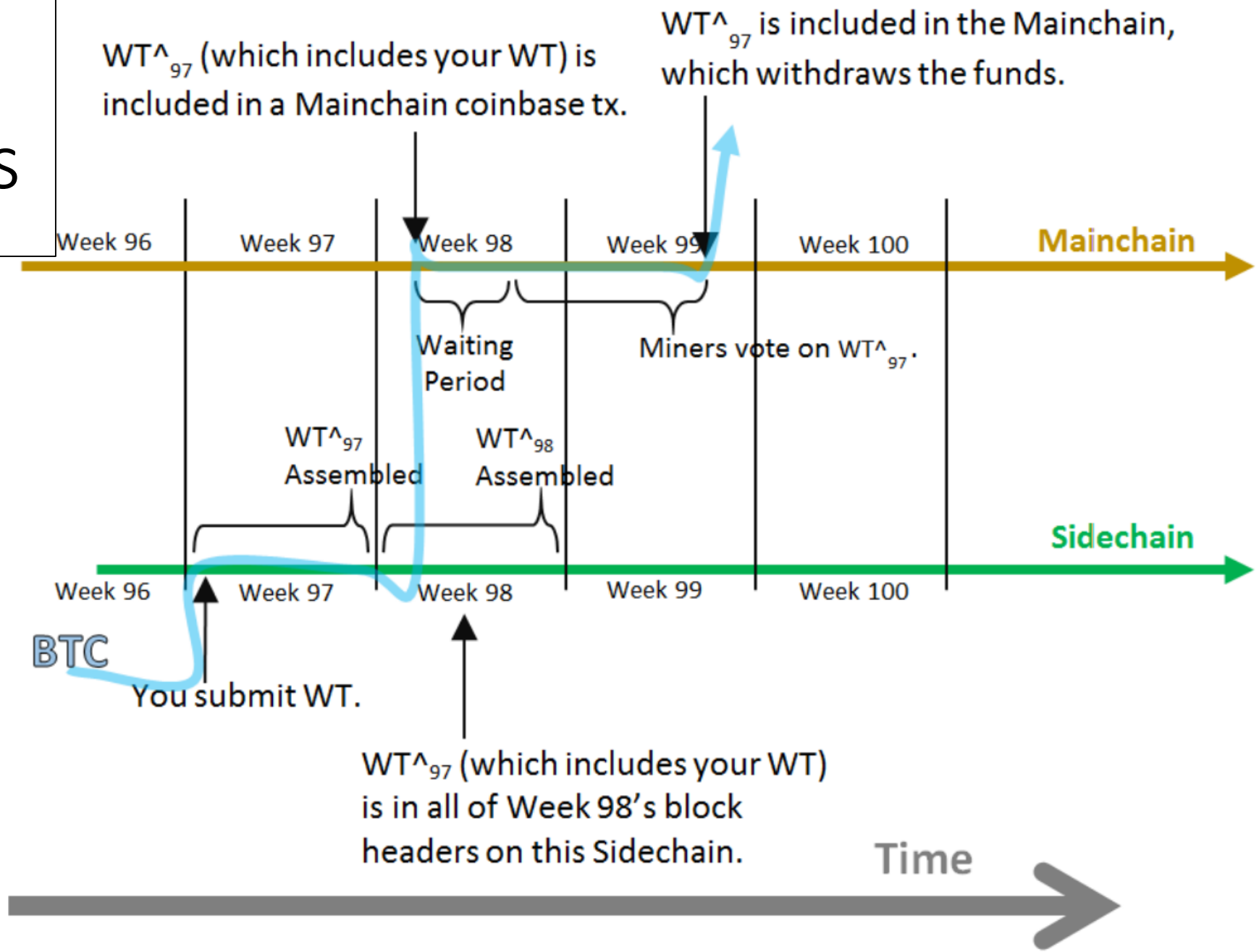
(You deposit 10 Core-BTC into RSK, making it 10 Ethereum-BTC. But will anyone willingly give you 10 Core-BTC for Eth-BTC?)
(We want all the Altcoin-related price risk to be hedged away.)

Drivechain -- Long Slow Transparent Vulnerable Withdrawals

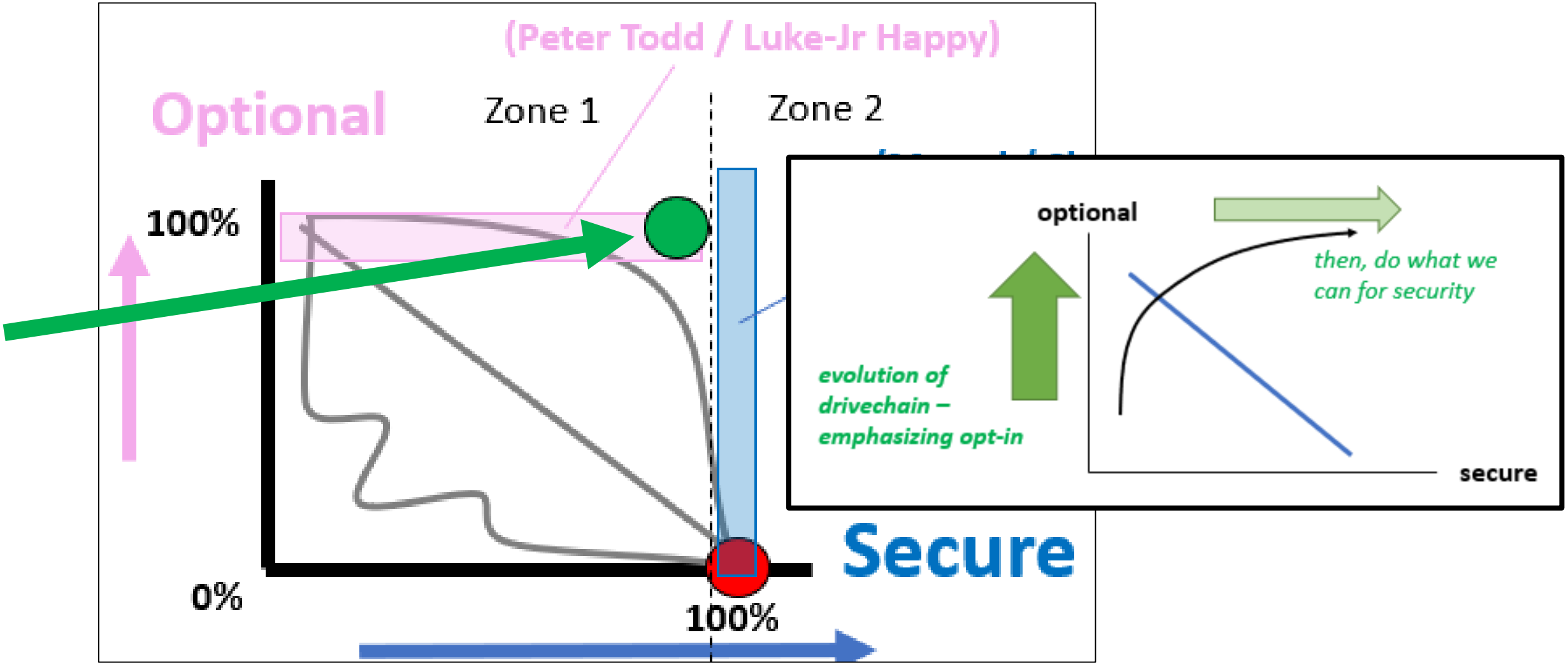


- **Slow**, *at least* 3 months, but pegged (1:1 rate).
- Recall, users get speed elsewhere:
  - main-to-side "deposits" via Embedded Consensus
  - ((main→side), (side→main)) trades via atomic swaps.
  - Cross-chain LN
- Users shouldn't be using the slow withdrawals – equivalent to having a legal contract enforced. (Similar to "closing a LN channel" – only done if something goes wrong.)
- Batch the withdrawals.

Batch the Withdrawals



Part 3 – Security Model



Part 3 – Security Model

Bitcoin open source implementation of P2P currency

Posted by Satoshi Nakamoto on February 11, 2009 at 22:27

View Discussions

I've developed a new open source P2P e-cash system called Bitcoin. It's completely decentralized, with no central server or trusted parties, because everything is based on crypto proof instead of trust. Give it a try, or take a look at the screenshots and design paper:

Download Bitcoin v0.1 at http://www.bitcoin.org

needed to support the company make micropayments impractical.

Bitcoin's solution is to use a peer-to-peer network to check for double-spending. In a nutshell, the network works like a distributed timestamp server, stamping the first transaction to spend a coin. It takes advantage of the nature

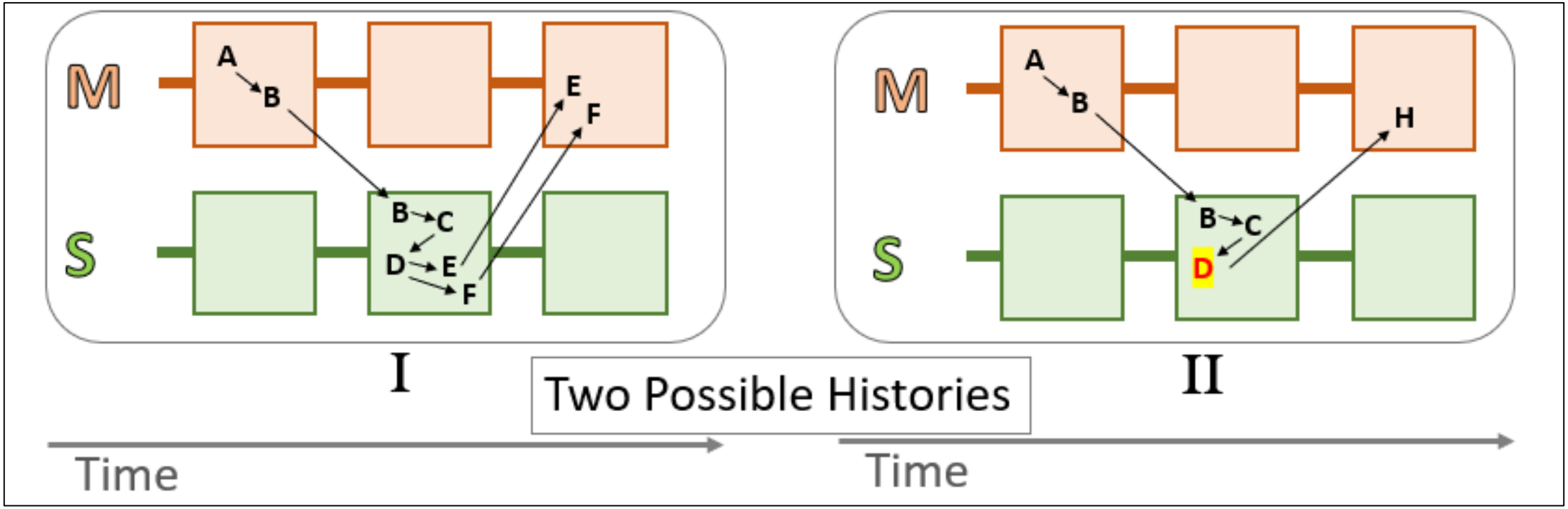
information being easy to spread but hard to stifle.

Only b/c PoW

Instead, Drivechain condenses the from-extension-to-original messages into infrequent, easy to validate, unambiguous, chain-scale messages. It essentially flips the consensus threat on its head by arguing that the sidechain should do all of the consensus labor, and it should then present a tiny, minimal easy-to-verify proof of that labor to the mainchain at infrequent intervals. (In the sense of being "difficult to generate but easy to verify", it resembles proof-of-work itself.) This allows us to solve problem [2] without compromising on [1]

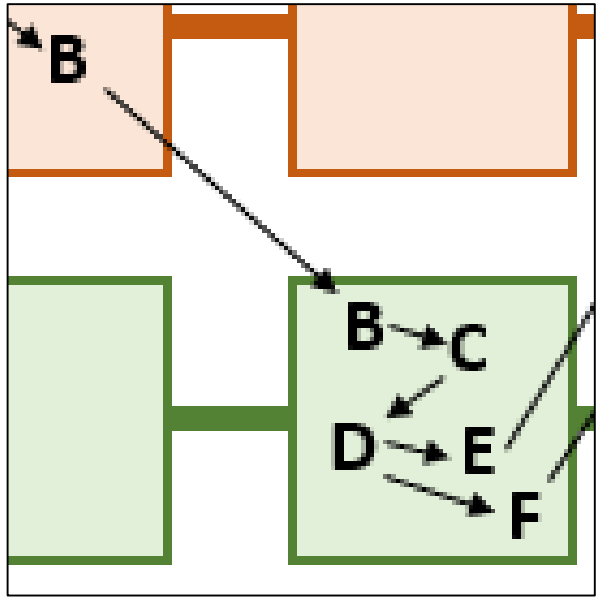
From: drivechain.info/faq

Remember Our Example?



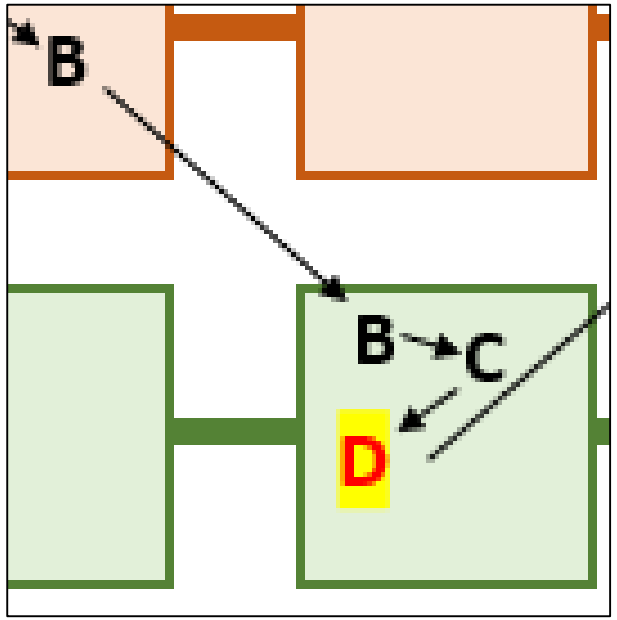
All Aboard!!

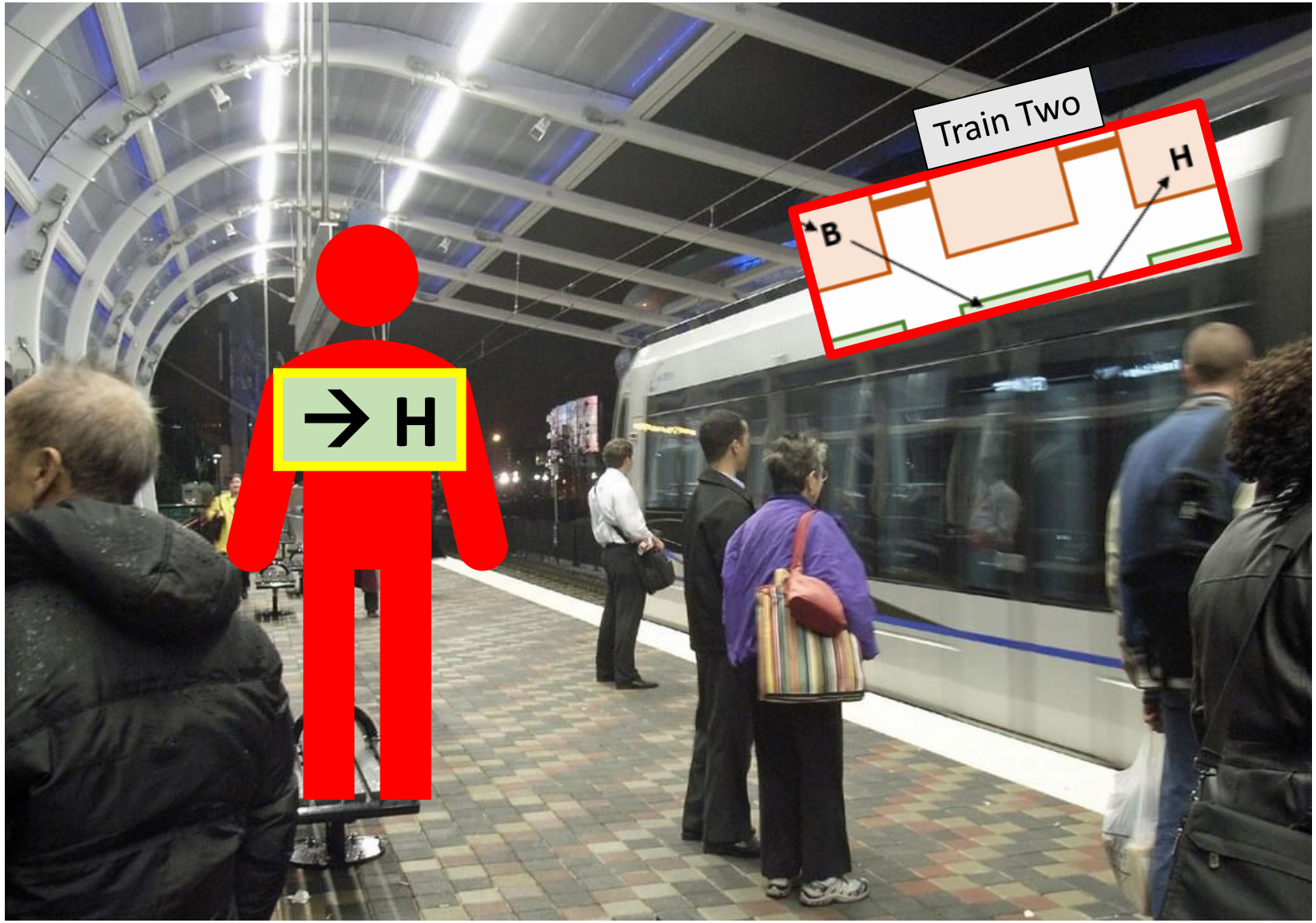
Remember…?



All Aboard!!

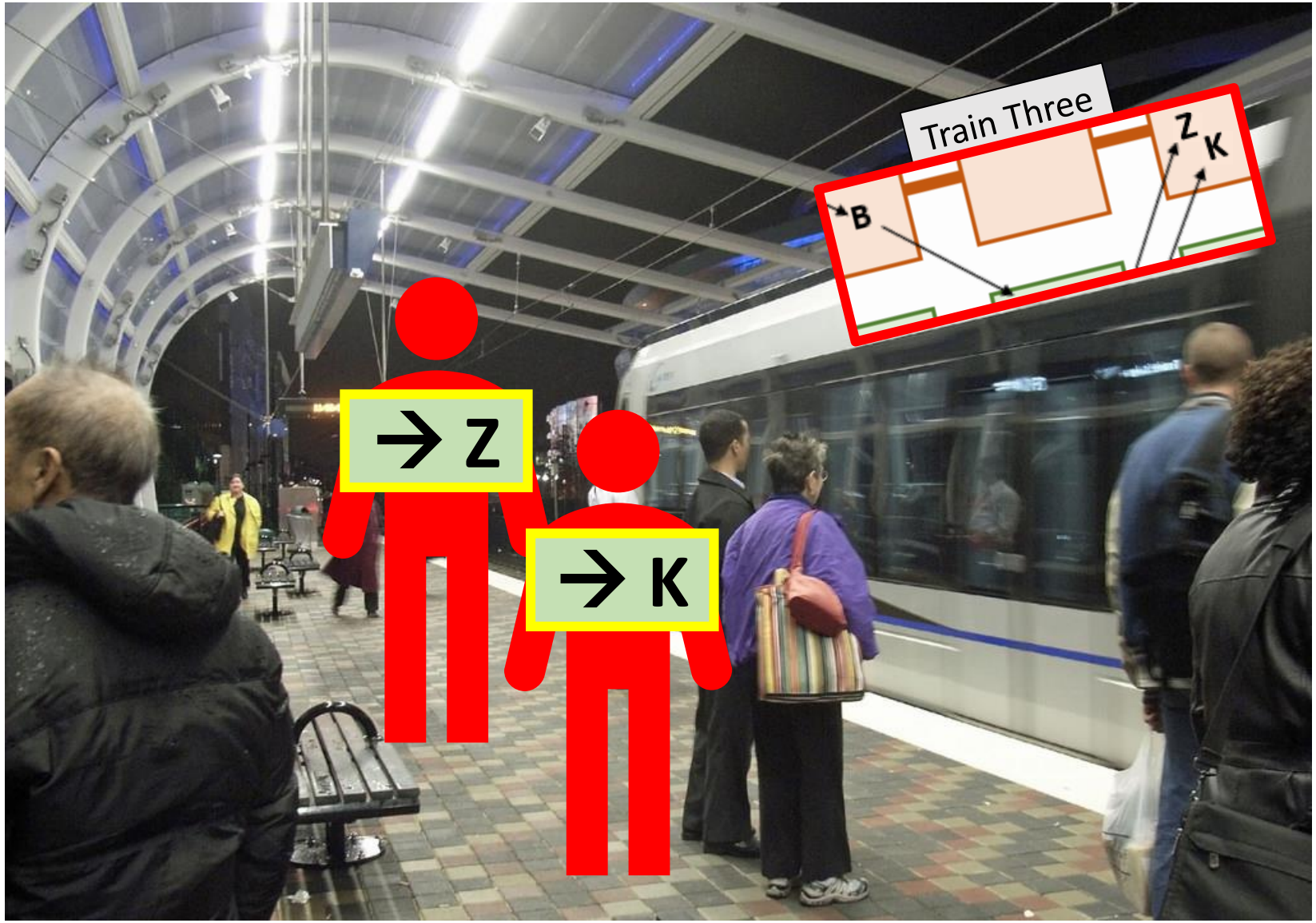
And also…?





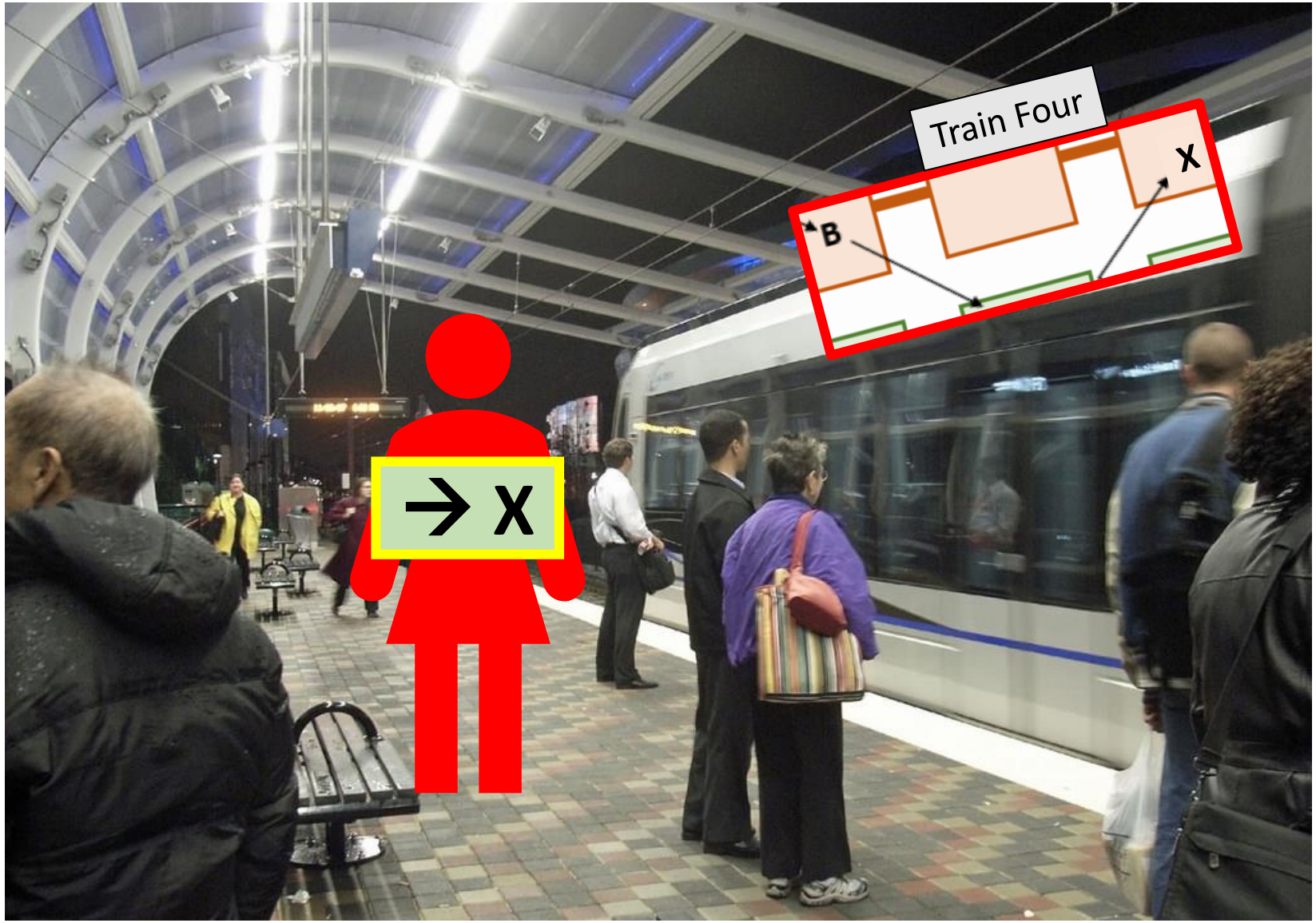
All Aboard!!

Another Theft-Attempt



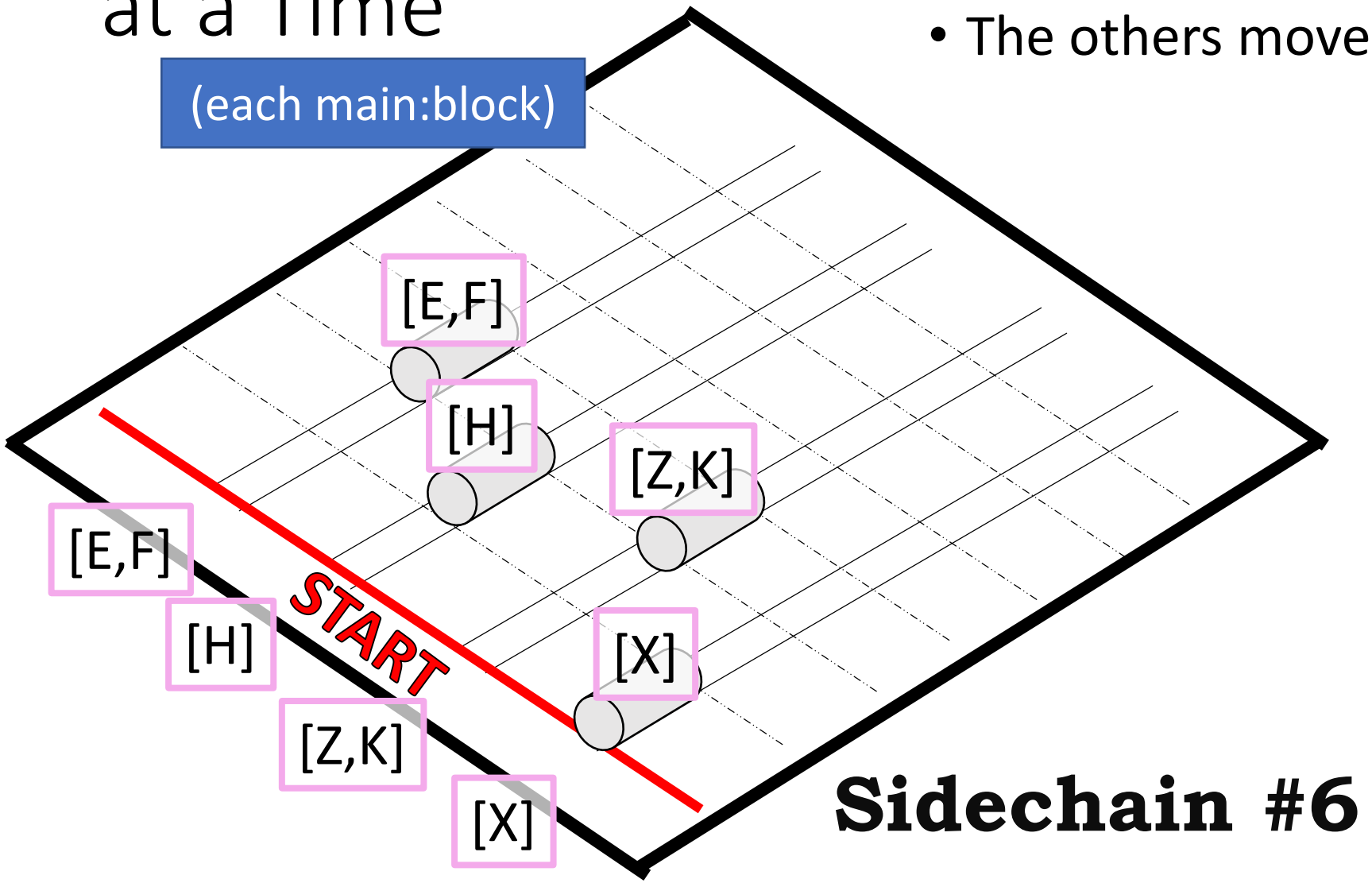
All Aboard!!

A third theft-attempt



Per Sidechain, Only One Traincar can advance at a Time

- The others move back.

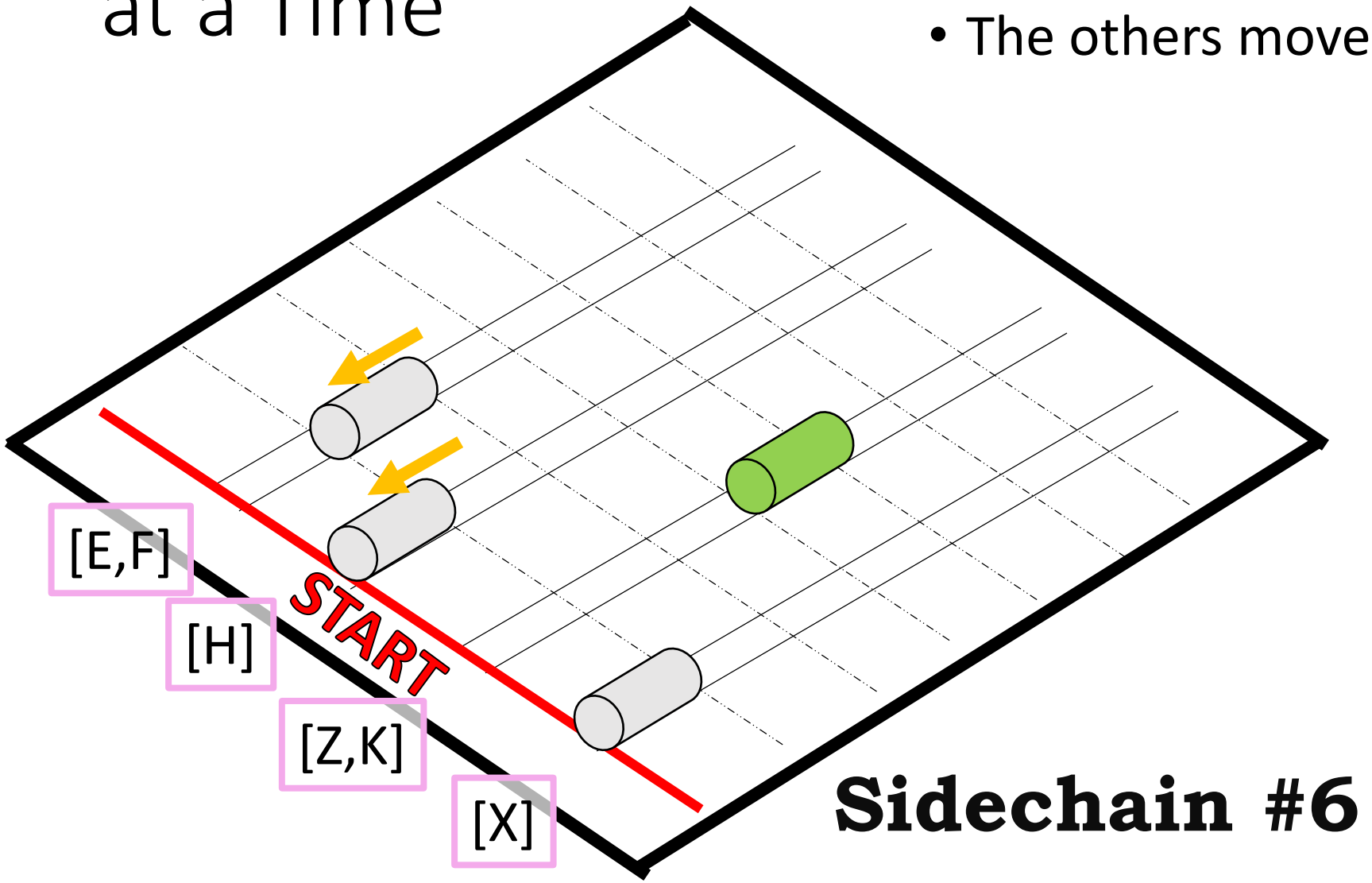


t = 9

Through t=16

Per Sidechain, Only One Traincar can advance at a Time

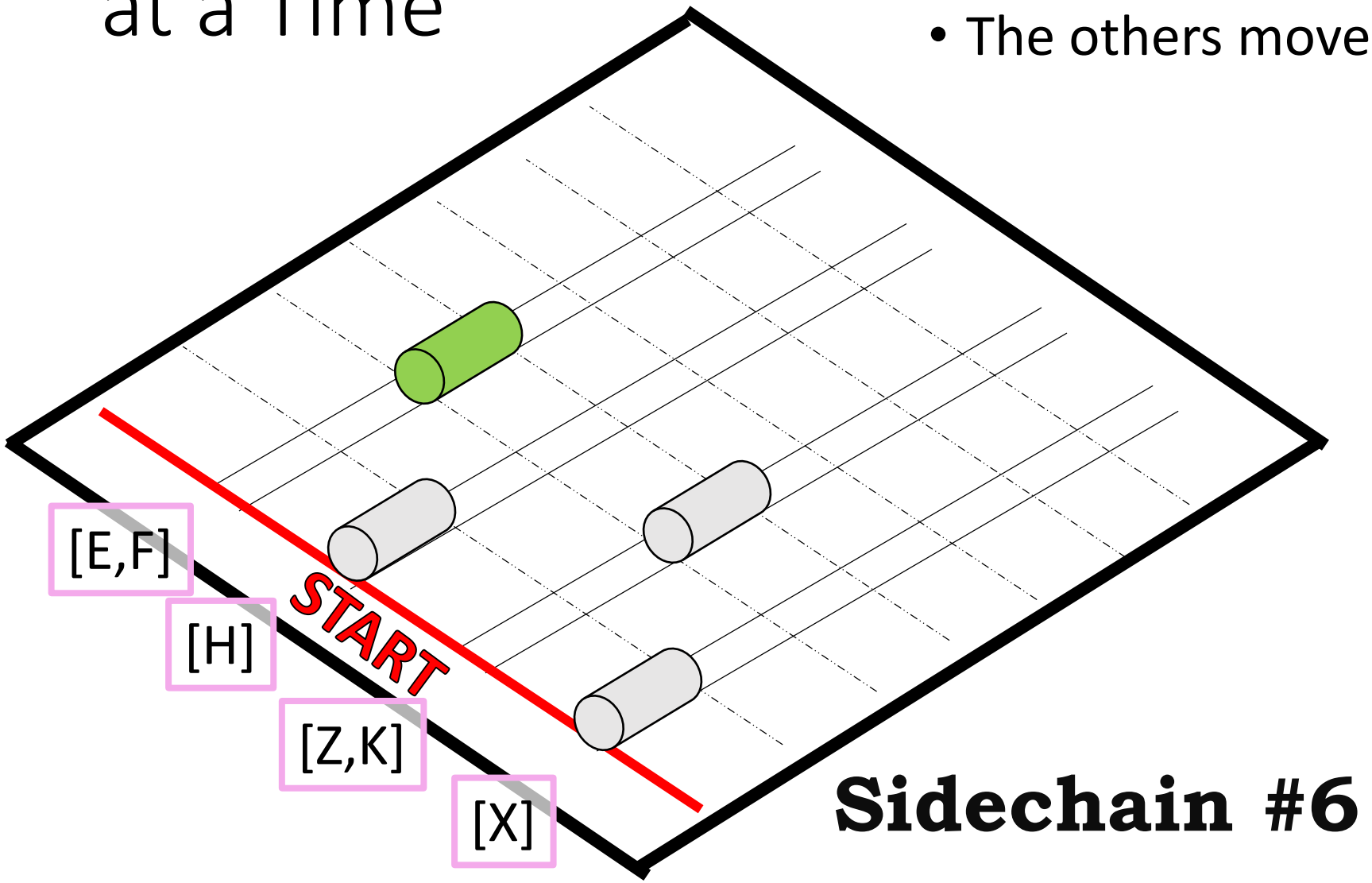
- The others move back.



t = 10

Per Sidechain, Only One Traincar can advance at a Time

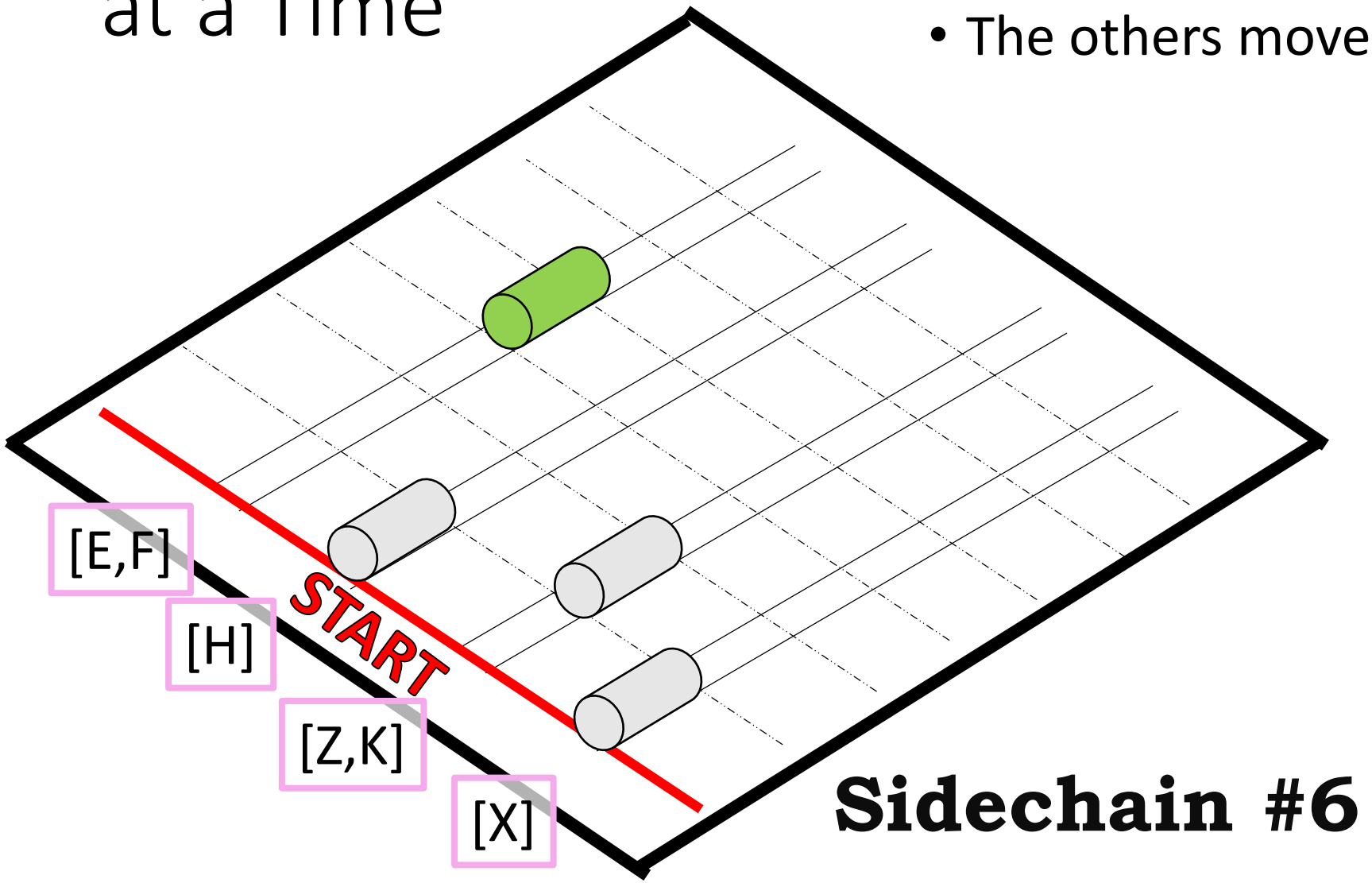
- The others move back.



t = 11

Per Sidechain, Only One Traincar can advance at a Time

- The others move back.



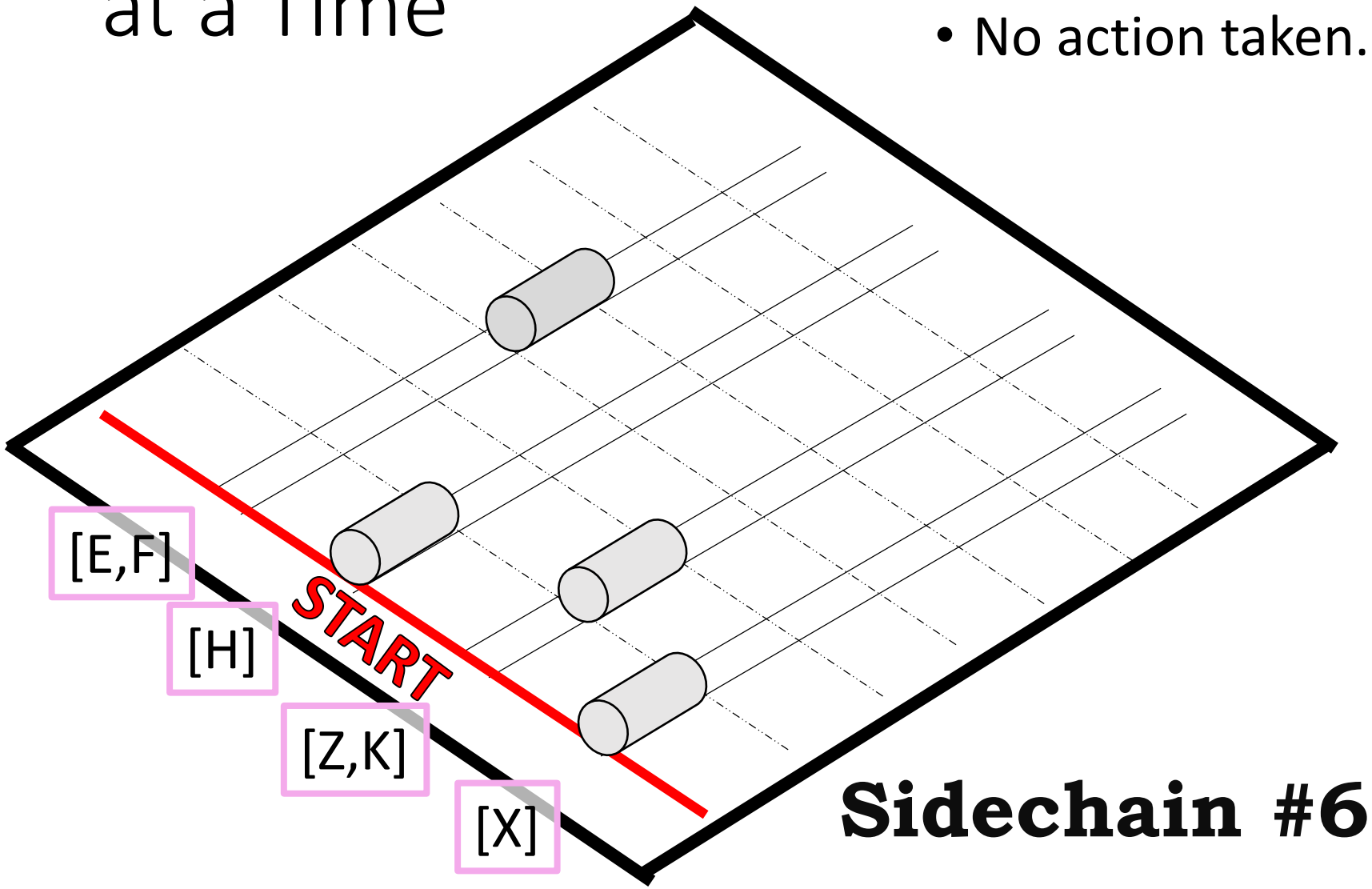
t = 12

Per Sidechain, Only One Traincar can advance at a Time

- No action taken.

Abstain

t = 13

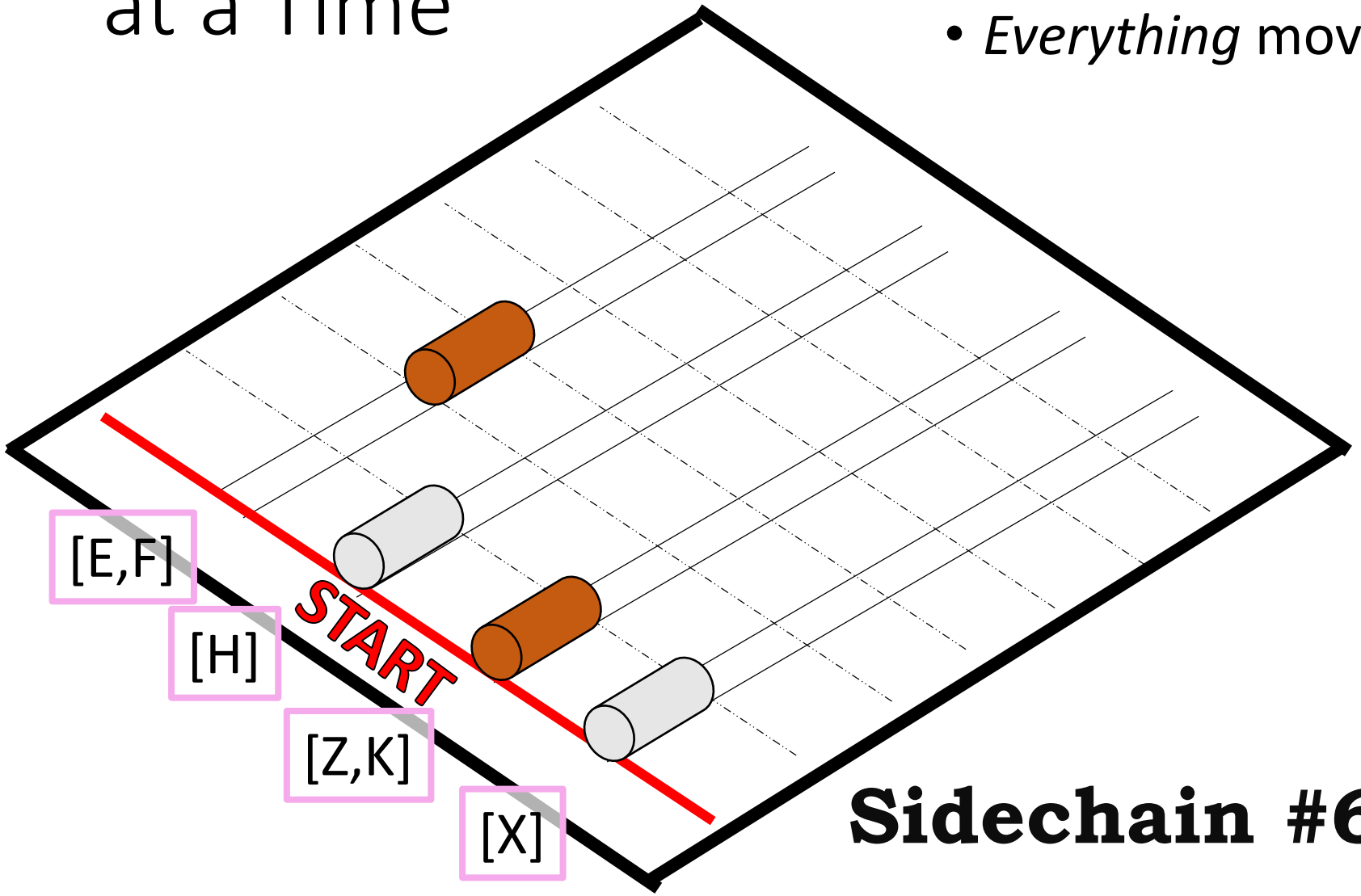


Per Sidechain, Only One Traincar can advance at a Time

- *Everything* moves back.

Alarm

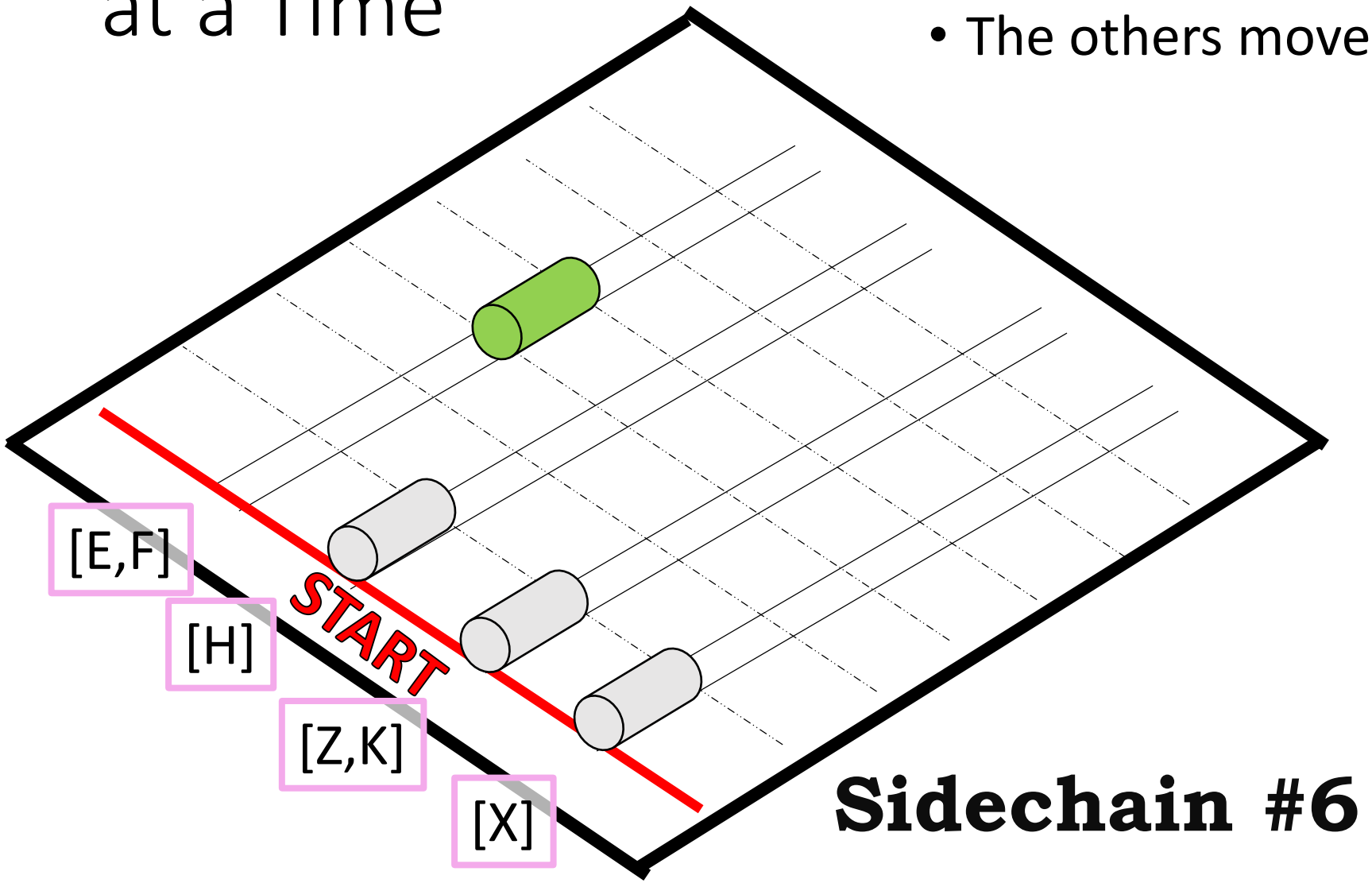
t = 14



Sidechain #6

Per Sidechain, Only One Traincar can advance at a Time

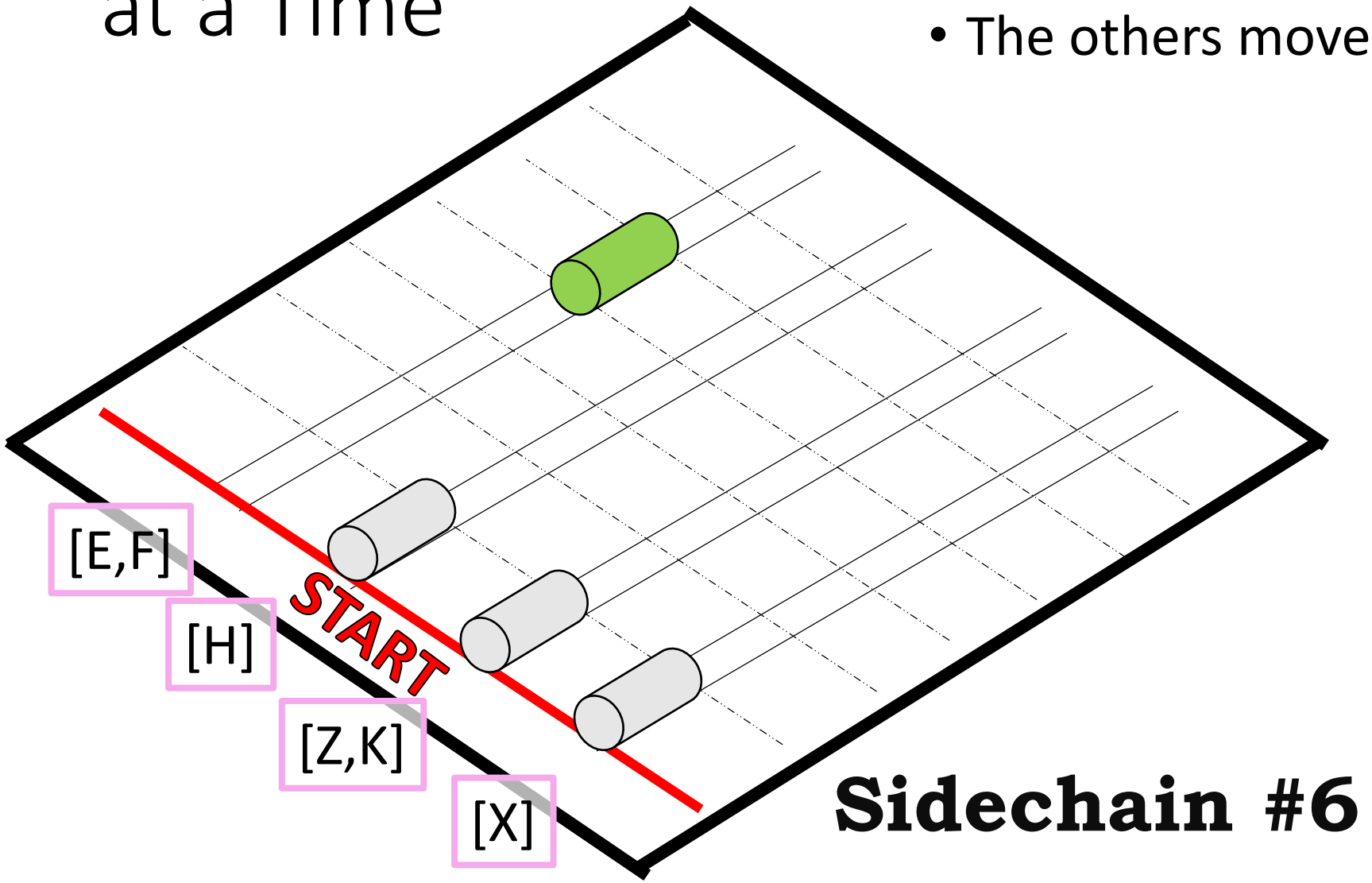
- The others move back.



t = 15

Per Sidechain, Only One Traincar can advance at a Time

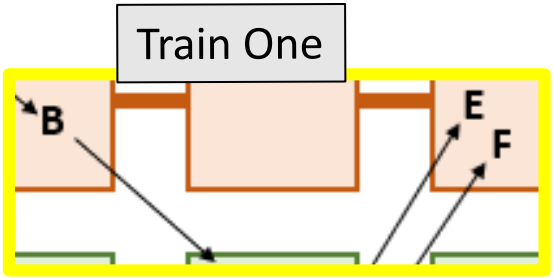
- The others move back.

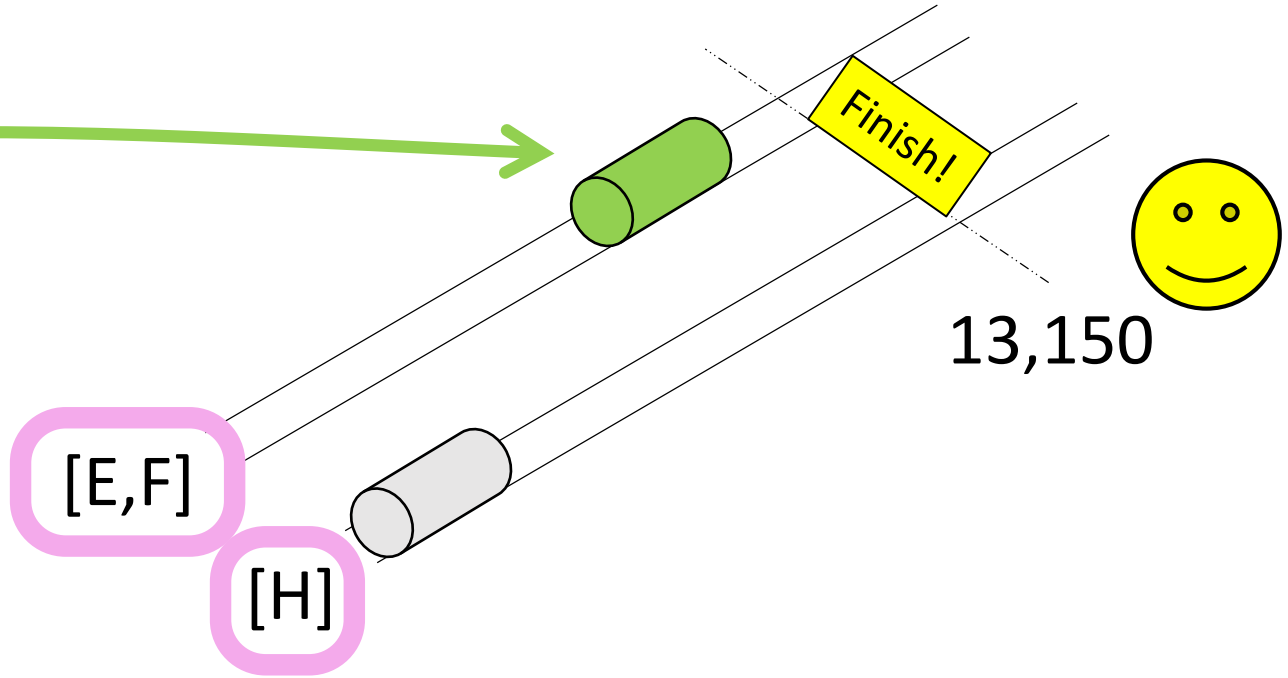


t = 16

Finish Line = Withdraw BTC

- If a train car advances 13,150 places (3 months confs) → '**finish line**'
  - **"Passengers"** can **"disembark"**.
  - *"Its txns"* can *"be included [in a main:block]"*.
  - BTC has moved from sidechain to mainchain, finally.
- Trains "expire" after 26,300 blocks (6 months).



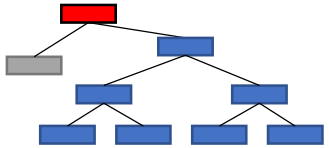


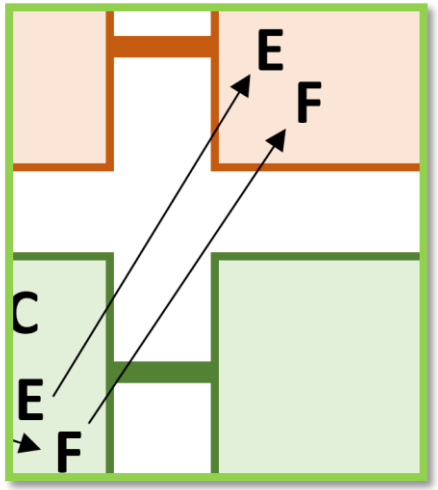
- **This info** is now "costly" to make, but *easy to verify* (next slide). Just like PoW.
- This is a de facto "SPV Proof" – the best so far.

Easy to Verify

Many ways to do it, DC won't force a particular way...because it can't (remember the veil).

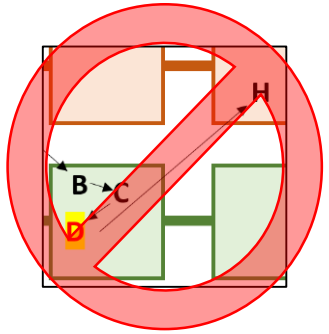
- Meanwhile, sidechain should make it **very** easy to learn **the "correct" withdrawal**.
  - Include it in *every* sidechain header (for 6 months).
  - Include it as the left node in a compound Merkle tree.





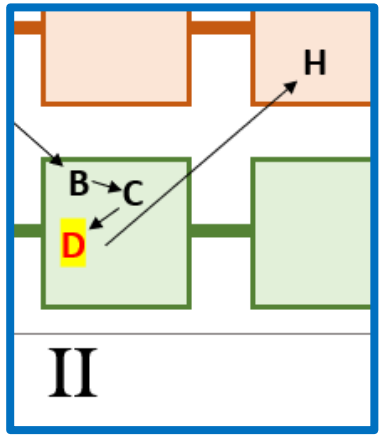
- Recall: mainchain has no idea which withdrawals are side:valid.
- But (disinterested) main:users and main:miners can still:
  1. Run sidechain in SPV mode, and examining the withdrawals there for stability and consistency.
  2. "Ask a friend" who runs this sidechain.
  3. Social proof – look at reputable authorities, social media.
  4. Use the Alarm (mentioned earlier).

But, no idea which headers are valid

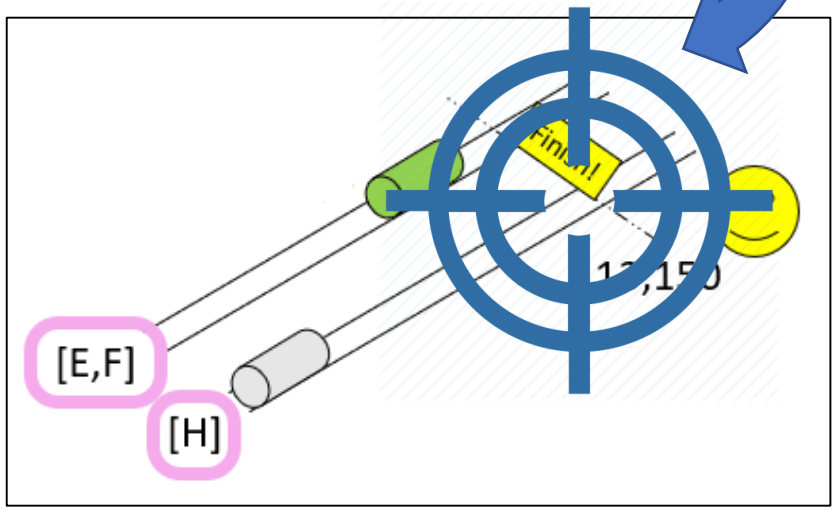


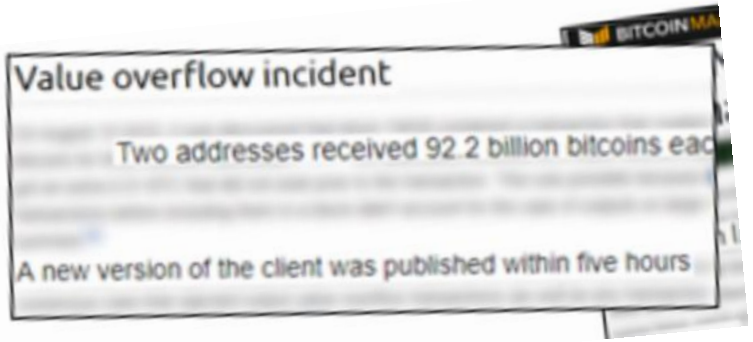
Full Sidechain Node	Drivechain "Monitoring"	Improvement Factor
2 GB per week (assuming current [1,4] MB limits)	One "bit" per 3 months (in equilibrium case)	192,000,000

The UASF Defense [and threat of]

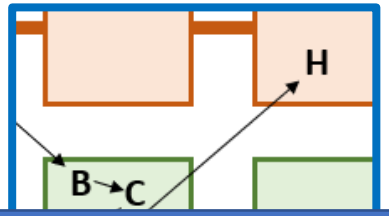


- If users detect a ***bad withdrawal***, they can choose to reject any block that includes it. (Ie, train arrives, but the doors don't open, and passengers aren't allowed to disembark.)
- Plans to make this **very easy in the UI** – just a few clicks. (+Box: Danger if not joined my economic majority.)
- Users can take their time, and will **never be surprised**. Takes 1+ month to advance 4,000 spaces, which is (1/3) the required distance. – Compare to V.O.I. and March 2013 HF.
- Miners don't know if users plan to UASF-defend, until they do it (ie, users automatically bluff for free).
- Since it won't accomplish anything, why bother attacking? If zero attacks, it is free to defend. Ideal!





The **UASF Defense** [and threat of]



Eric Lombrozo and 20 others follow

I, Troll @brian_trollz · Jan 21

Replying to @CryptAxe @Weathermanlam

Drivechains/Mined Sidechains have a security flaw so far in that they count on social coordination as a check against miners maliciously updating state. This is a paradox, as mining IS the method of social coordination to update state.

2 1

Previous "Paradoxes"

Bitcoin Network Shaken by Blockchain Fork

by **Vitalik Buterin**

Mar 12, 2013 11:14 PM EST

Yesterday, the Bitcoin network experienced one of the most serious hiccups that we have seen in the past four years. Starting from block 225430, the blockchain literally split into two, with one half of the network adding blocks

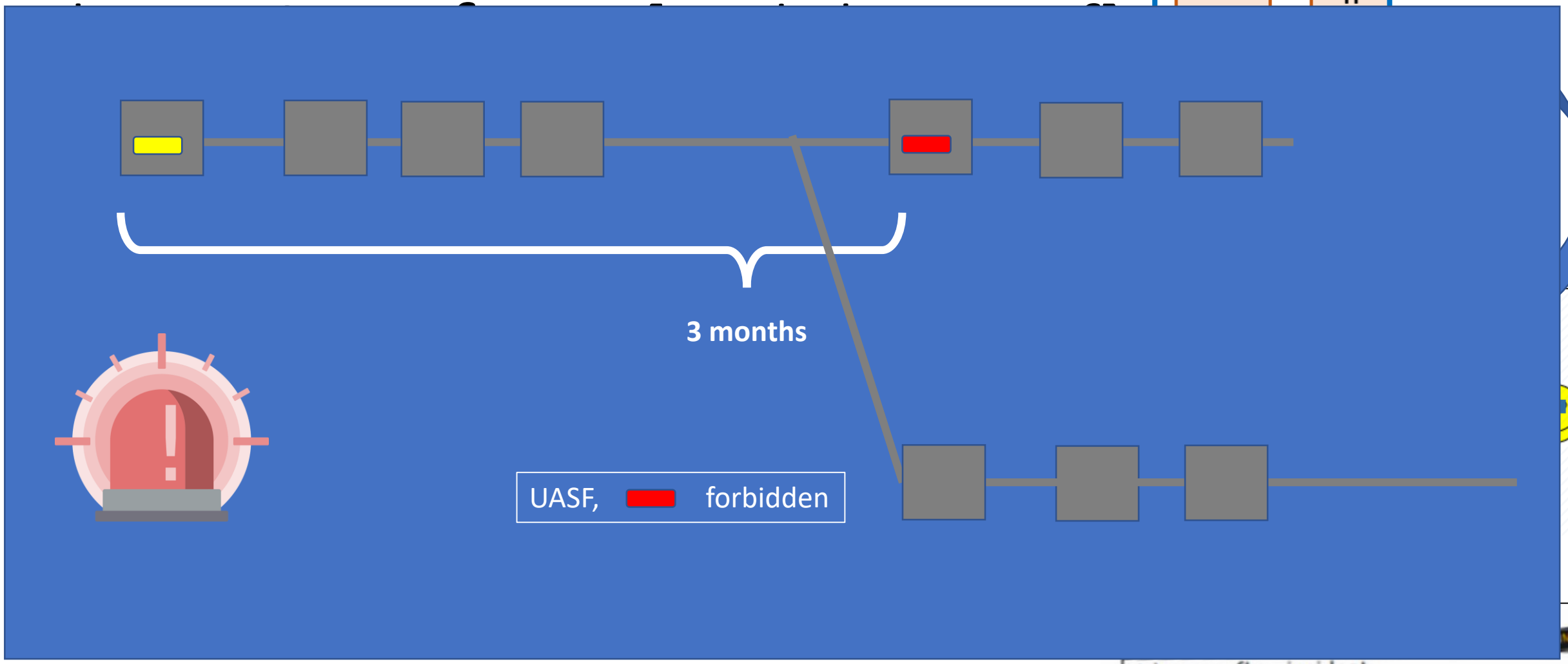
The split

Value overflow incident

Two addresses received 92.2 billion bitcoins eac

A new version of the client was published within five hours

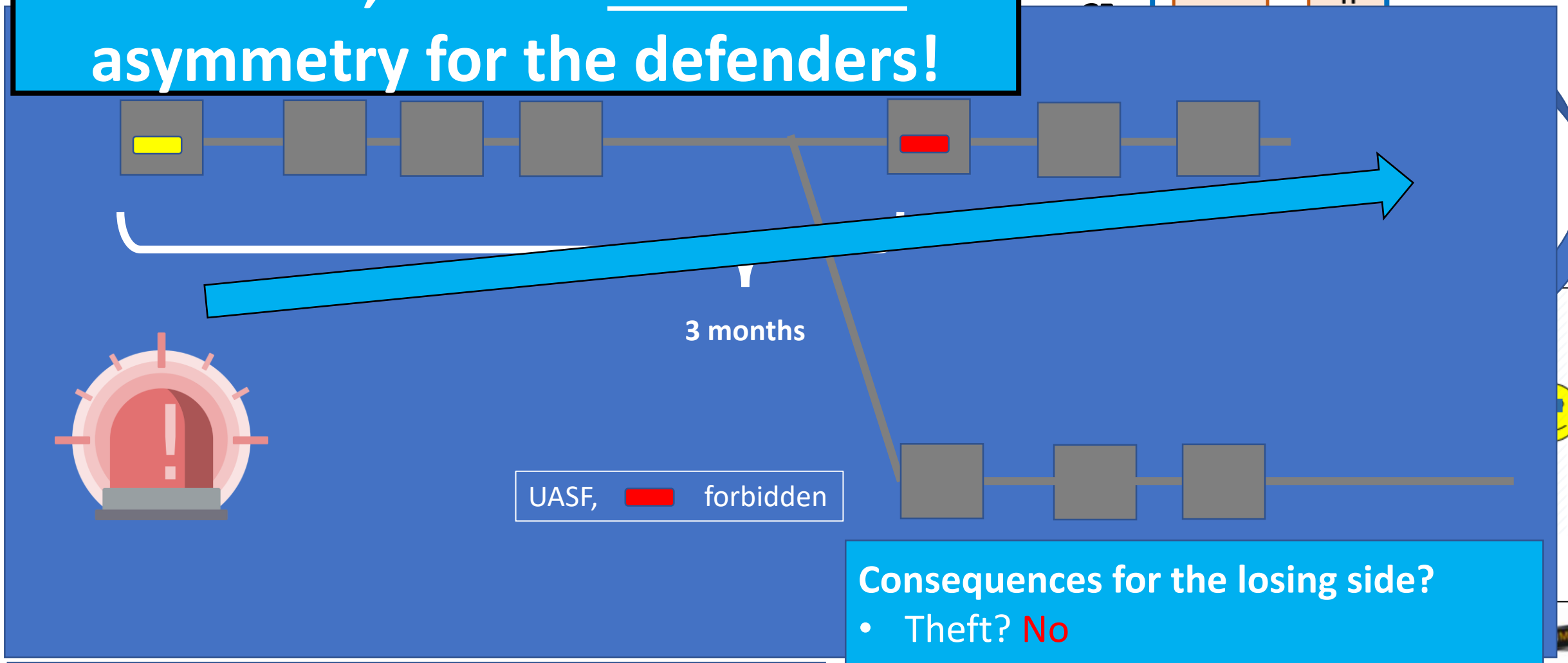
Same Process, but: 5-6 hours after vs 3 months before



- Since it won't a
  If zero attacks,

UASF Timeline

But wait, there's *even more* asymmetry for the defenders!



Failed UASF?

Consequences for the losing side?

- Theft? No
- Can't Spend BTC? No
- Rollback? No – miners not here

→ …can't receive BTC until you give up.

Alphonse Pace
@AlpacaSW

Follow

Replying to @adam3us @Truthcoin and 17 others

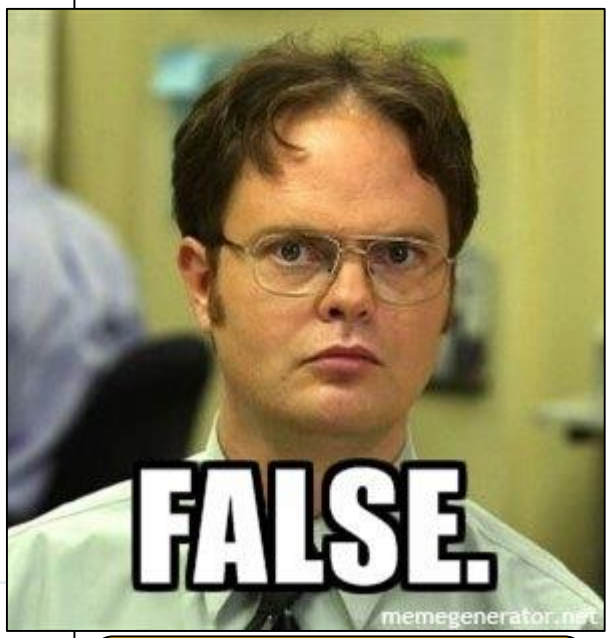
I'm not a fan of acting to appease ignorant people or attackers like the media. No bailouts if you bet wrong and lose. Media would have loved rollbacks of hacks too.

9:42 AM - 4 Feb 2018

3 Likes

2

Liked by Giacomo Zucco, CEO Blockchainlab.it



No Rollback

Miner Economics

- Miners -- incentive to maximize exchange rate.
- If sidechains good, activation → increase BTC price.
- Price increase → equilibrium difficulty increase.
- After difficulty increases to a certain point miners will *only* be able to remain profitable, if they have a 100% "support good sidechain" policy.

Does NOT mean they run sidechain nodes.
May just mean "alarm if there is ever more than one train"

A 51% Attack (Miner Centralization) – A Comparison

- Mainchain vs Sidechain vs LN -- FYI, I think all three ***are*** secure.
- With 51%, I would not attack the entire LN at once. I would attack via a *mosquito strategy* – where miners connect to LN-hubs and try to defraud <1% of the channels. Perhaps: 1 channel/day, or 1/hour.

	Regular Bitcoin	Drivechain	Lightning Network
Method of Theft:	Intentional large (6+ block) chain reorganization	Advance a dishonest withdrawal 13,150 times.	Broadcast an old channel state & refuse to include fraud proof.
Proving Fraud:	Automatic (You'll notice the reorg)	Easy (1 bit/3 months) -- DoS Resistant	Easy (auto-watch for valid, ultra-high fee, LN-channel-shaped txns)
Attack Requires 51% for…?	7+ blocks (70 +minutes)	13150 blocks (3 months) [reorg 7+ blocks 70 min]	1000+ blocks (1 week) [reorg 7+ blocks 70 min]
Affects:	All main and side chains.	All sidechains.	Single individual txn.
Will Others Care?	Yes	Probably	Probably Not
Recourse:	PoW Change (Hard)	UASF (Easy)	PoW Change (Hard)
If attack succeeds:	Exchange rate falls (unreliable network); Tx-Fees fall (lower demand)	E.R. falls (token no longer multi-chain); Tx-Fees fall (no SC fees)	E.R. falls (LN unsupported); On-chain txn fees rise.

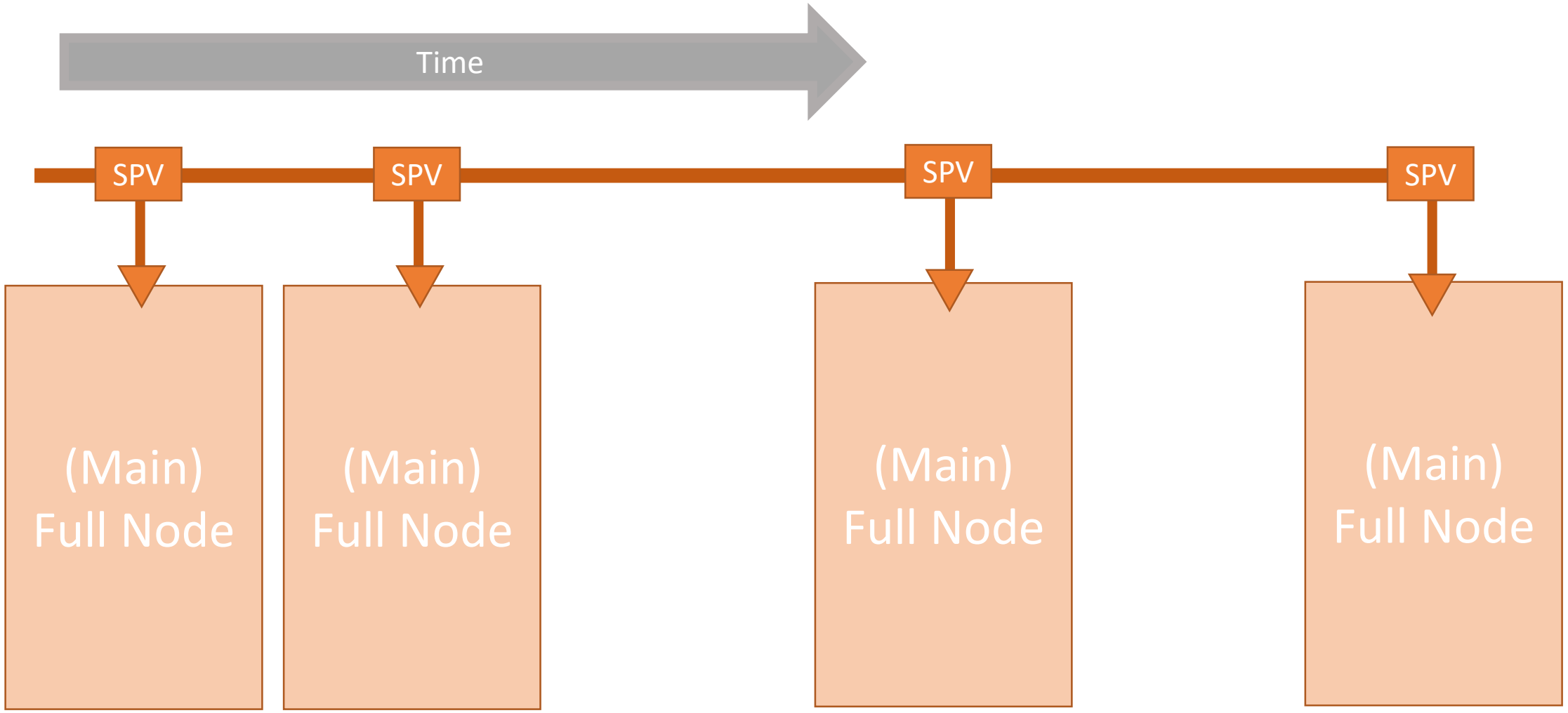
harassment

perverse incentive

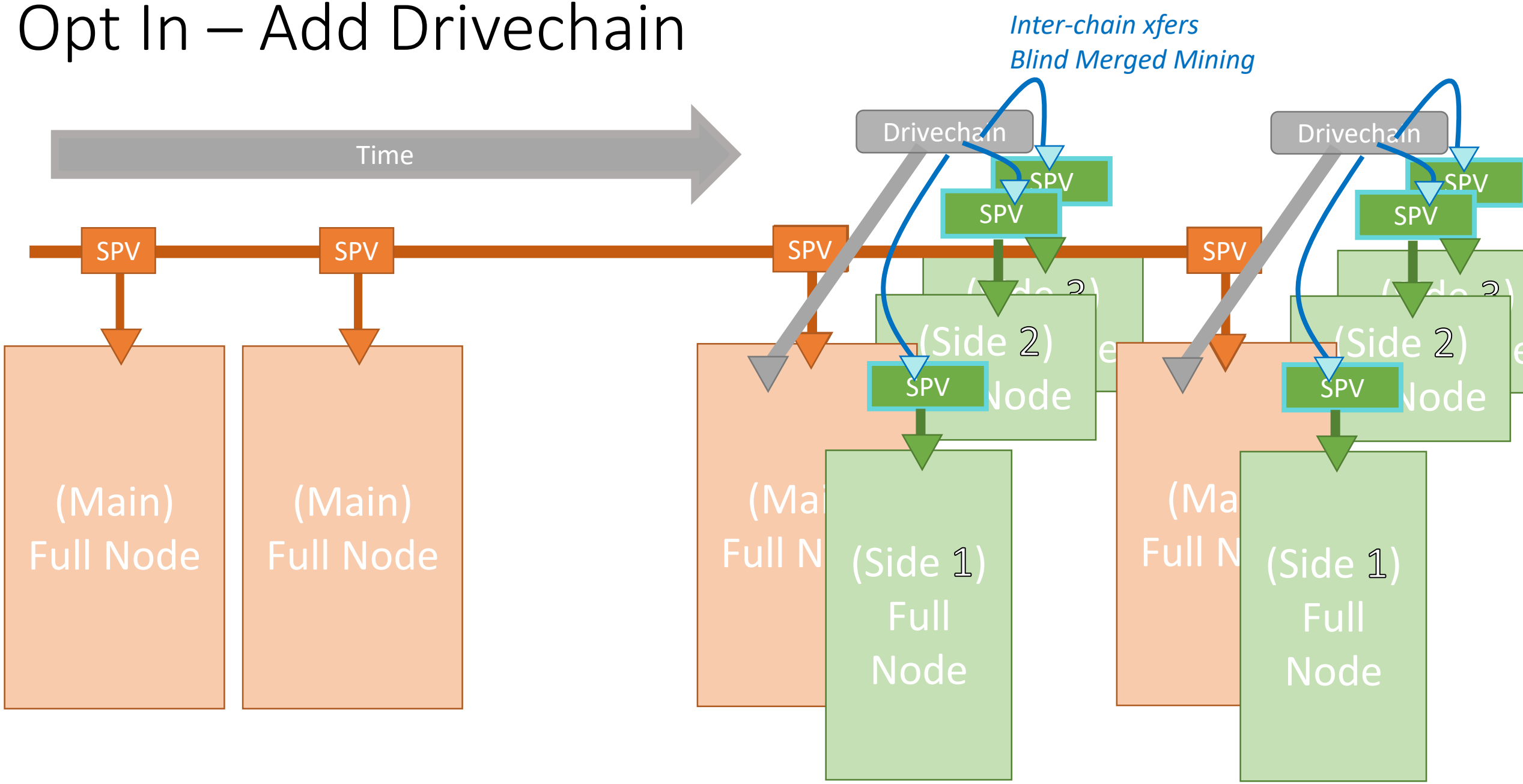
Part 4 – Blind Merged Mining

- Making Drivechain 100% opt-in, for miners as well as users.

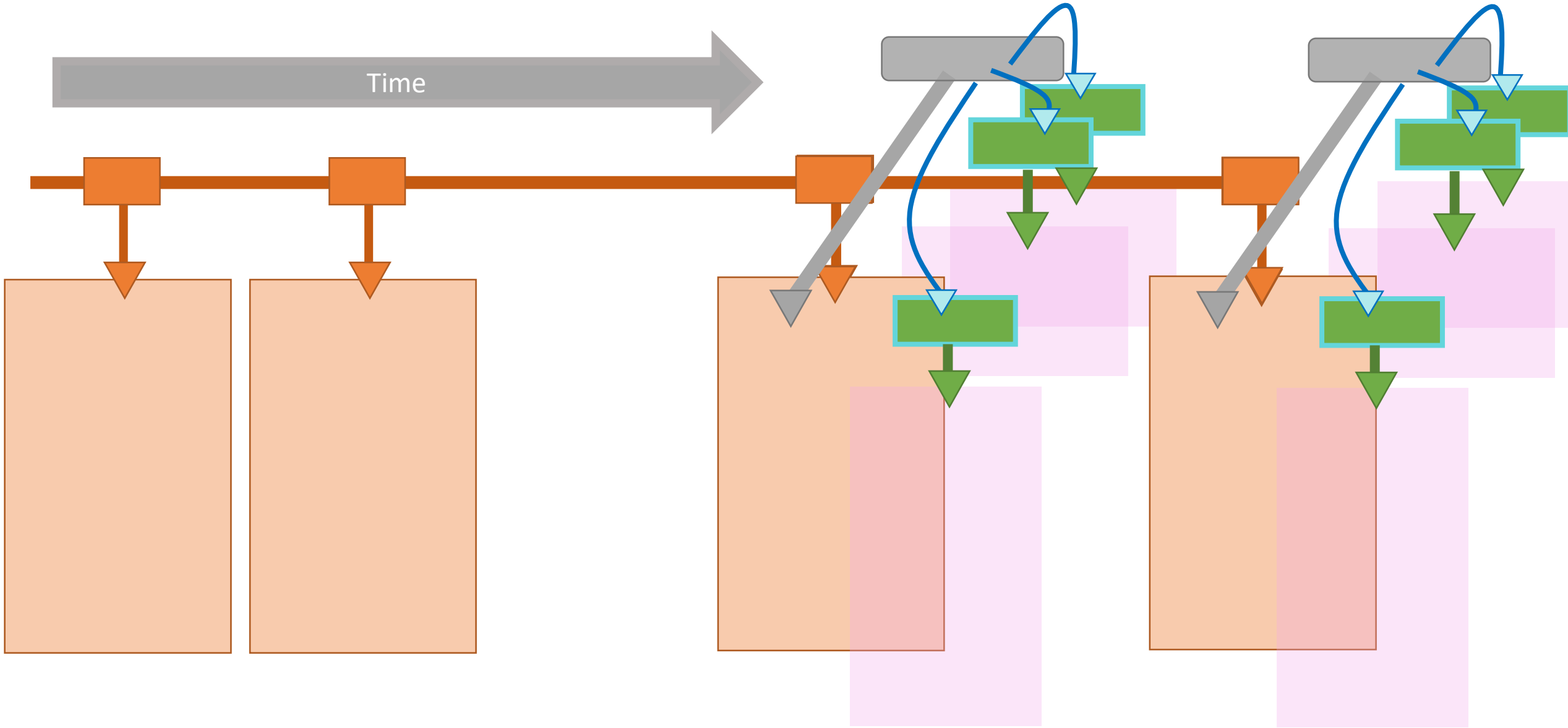
Drivechain: 100% Opt In, Yet Very Easily Secure



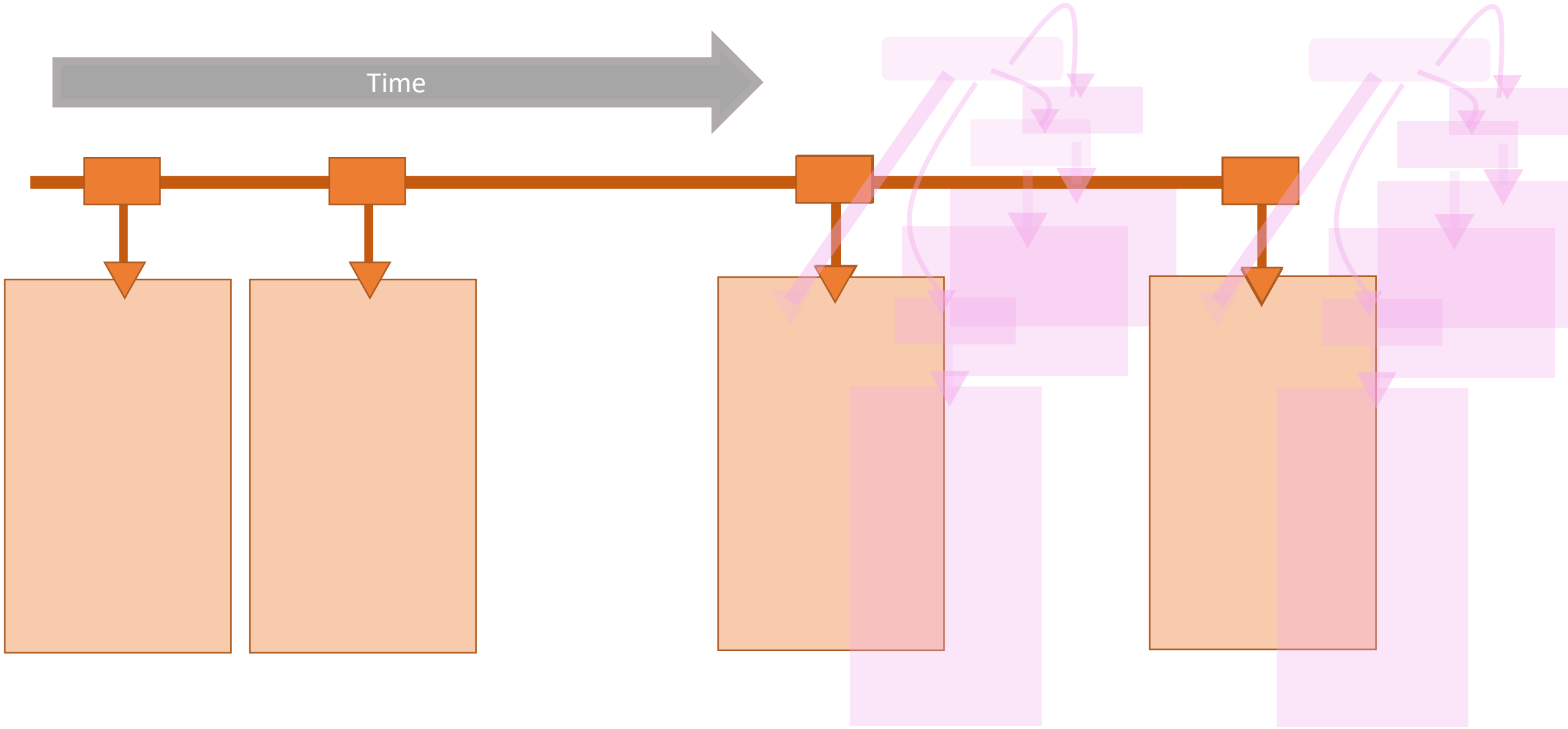
Opt In – Add Drivechain



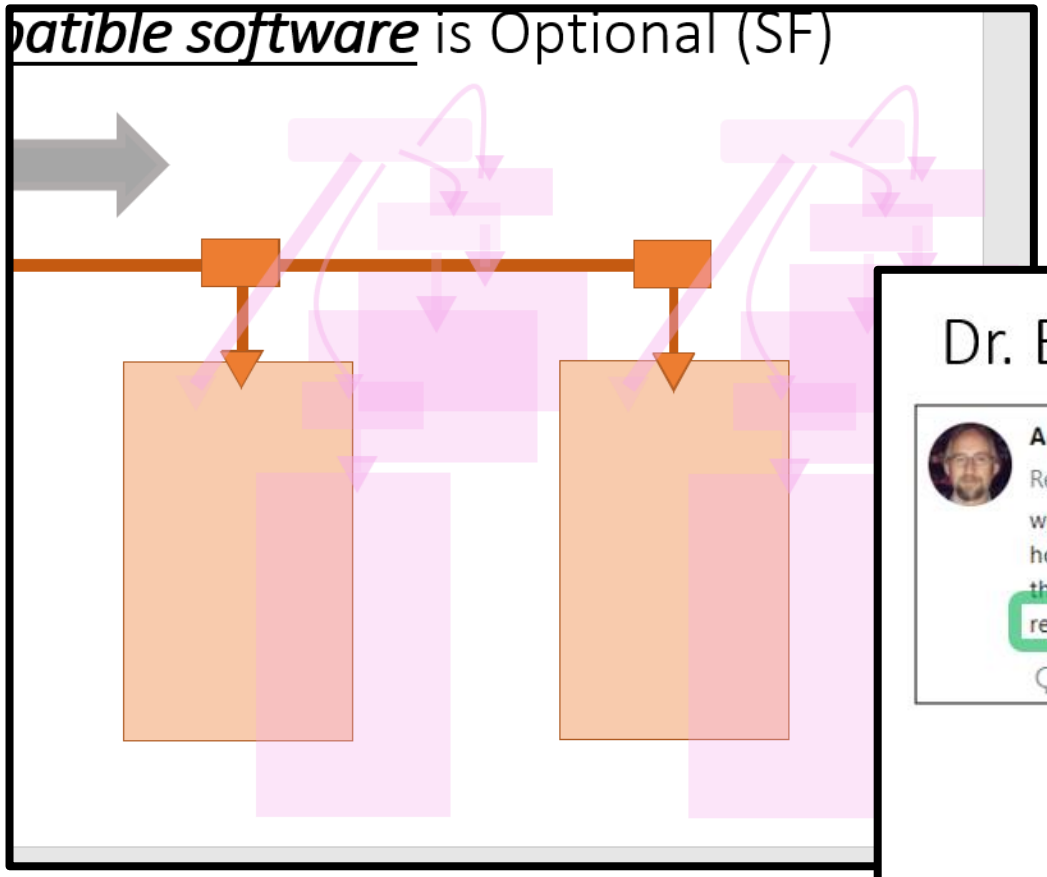
Opt In – **Sidechain Full Node** is Optional



Even ***Running DC-compatible software*** is Optional (SF)



This is Actually *Required* (Remember?)



Else, we regress to the extension block – which is an Evil Fork –mainchain FULL nodes ***must do more validation*** lest they become un-FULL.

Dr. B – Extension Block vs Drivechain

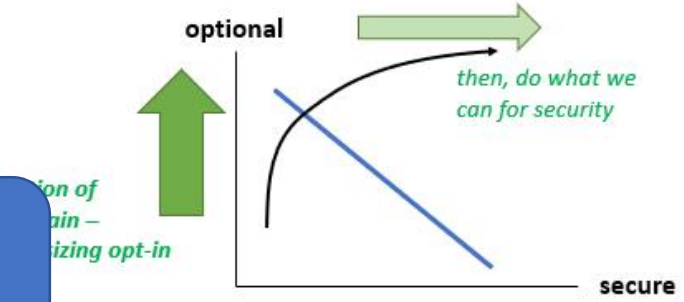
Adam Back @adam3us · 14 Nov 2017

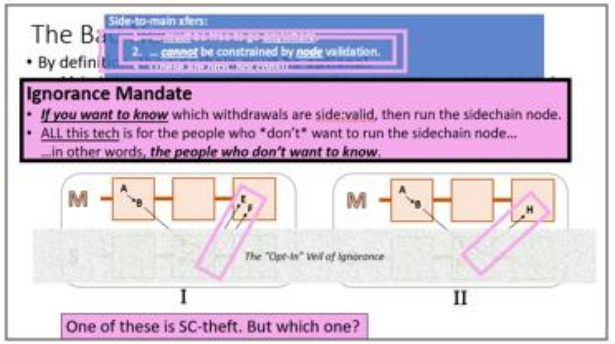
Replying to @Truthcoin @AlpacaSW

well it's not a free lunch though: ext-blocks externalise validation costs for bitcoin holders and users. I think people more prefer the **drivechain** approach, as then the code is not expanding consensus critical code, nor as directly increasing required data to validate main chain

1 2

Drivechain: mandatory trivialities (for miners). Optional everything (for users).





Ironically, ***problem*** with Extension Blocks is that miners can ***Never*** steal from them. At which point it becomes a full force consensus rule, and you are ***forced to know***.

Even ***giving people an option*** almost certainly can't have *any effect at all* … (let alone a negative one)!

List of cryptocurrencies

From Wikipedia, the free encyclopedia

is over 1384 and growing.[1] A new cryptocurrency
n network, followed by Ethereum, Ripple, Bitcoin

Cryptocurrencies [edit]

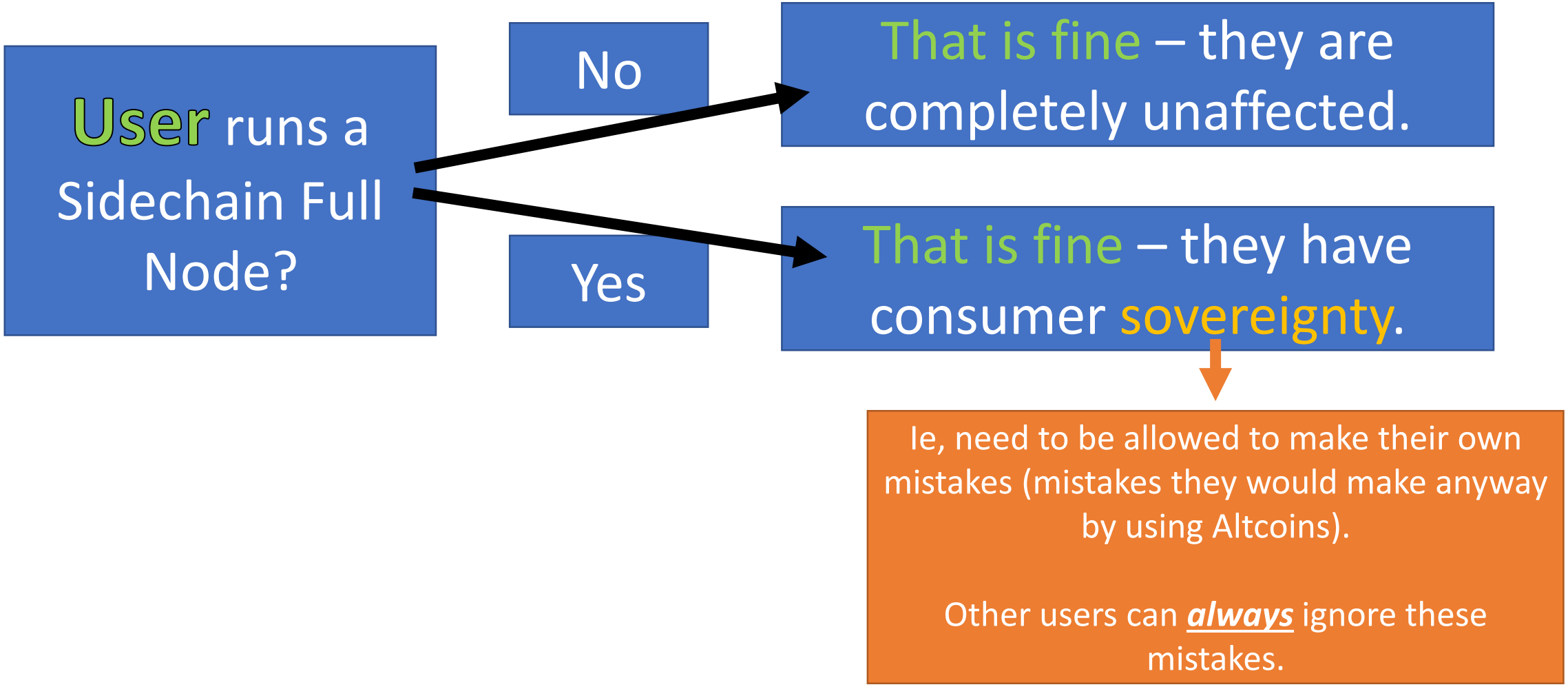
Belo

The number of cryptocurrencies available
is over 1384 and growing.

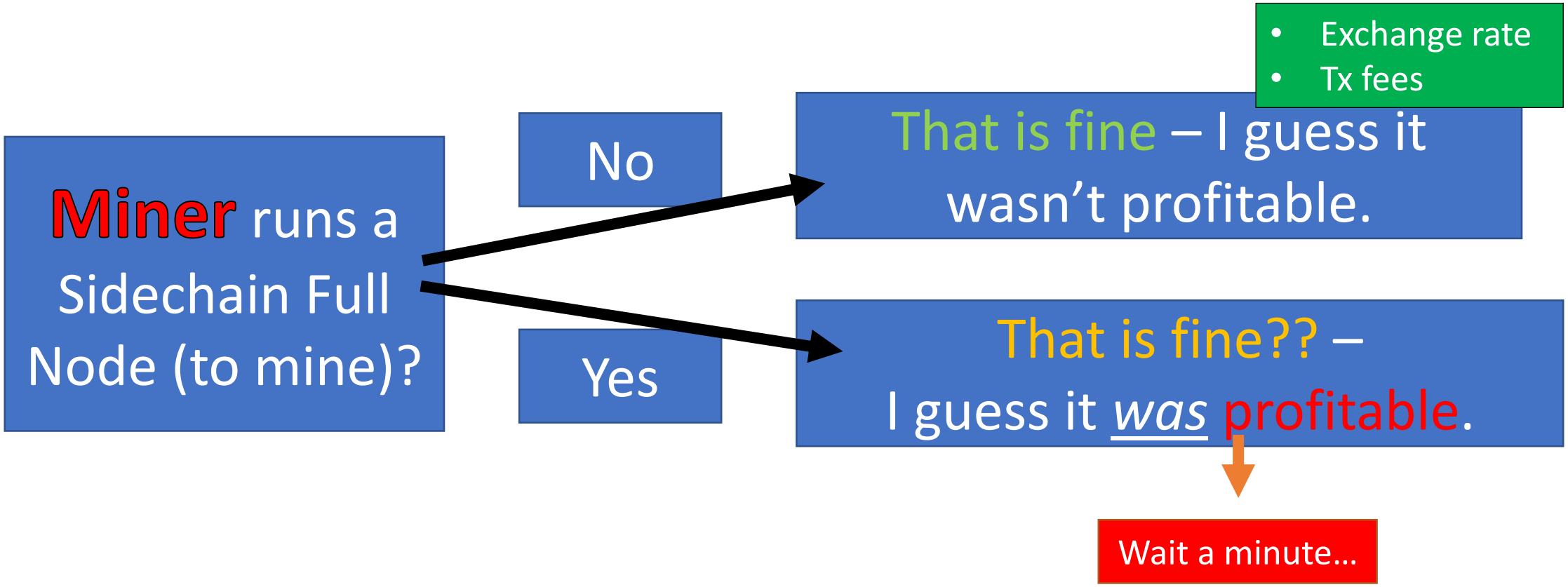
Rel							
200							notable and highest market capitalization.
2011	Active	Litecoin	LTC	Charlie Lee	Scrypt	PoW	The first cryptocurrency to use Scrypt as a

…because the ***Altcoins*** (and Spinoffs) *already* give users those options.

So, no criticism is really possible…

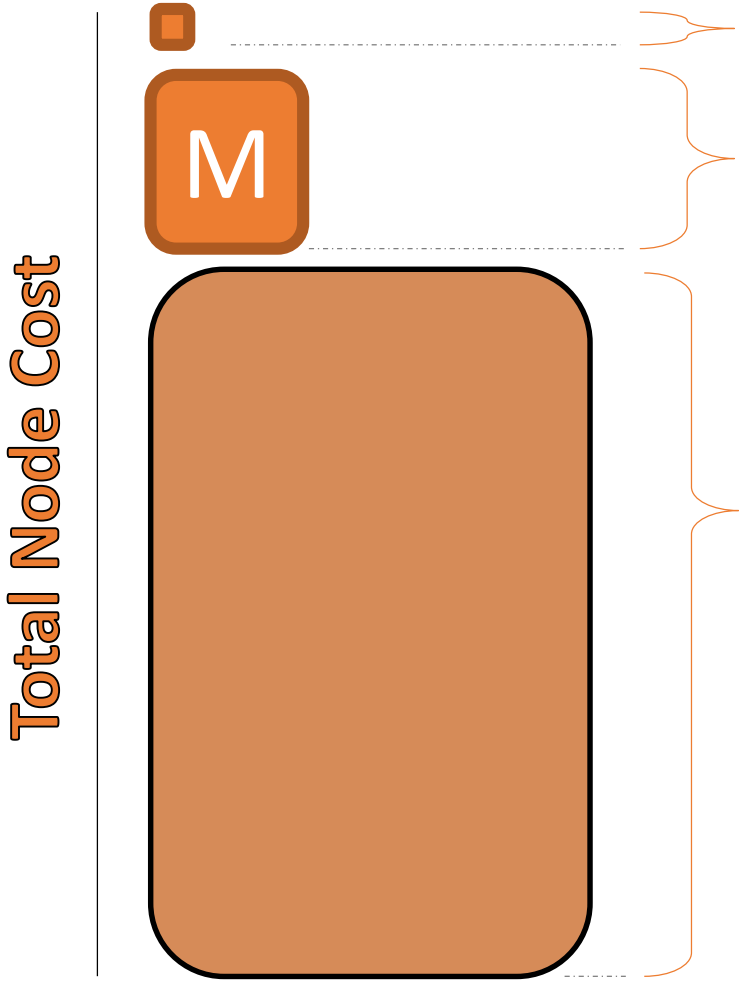


So, no criticism is really possible (?)…



Network Externalities

Miners Pay?



Cost of "outsourced validation"

Web wallet
Phone wallet

Always

Cost ($) of Full Node:

- Bandwidth
- Equip / CPU / Power
- Storage

Rarely

Externality Full Node Cost ($):

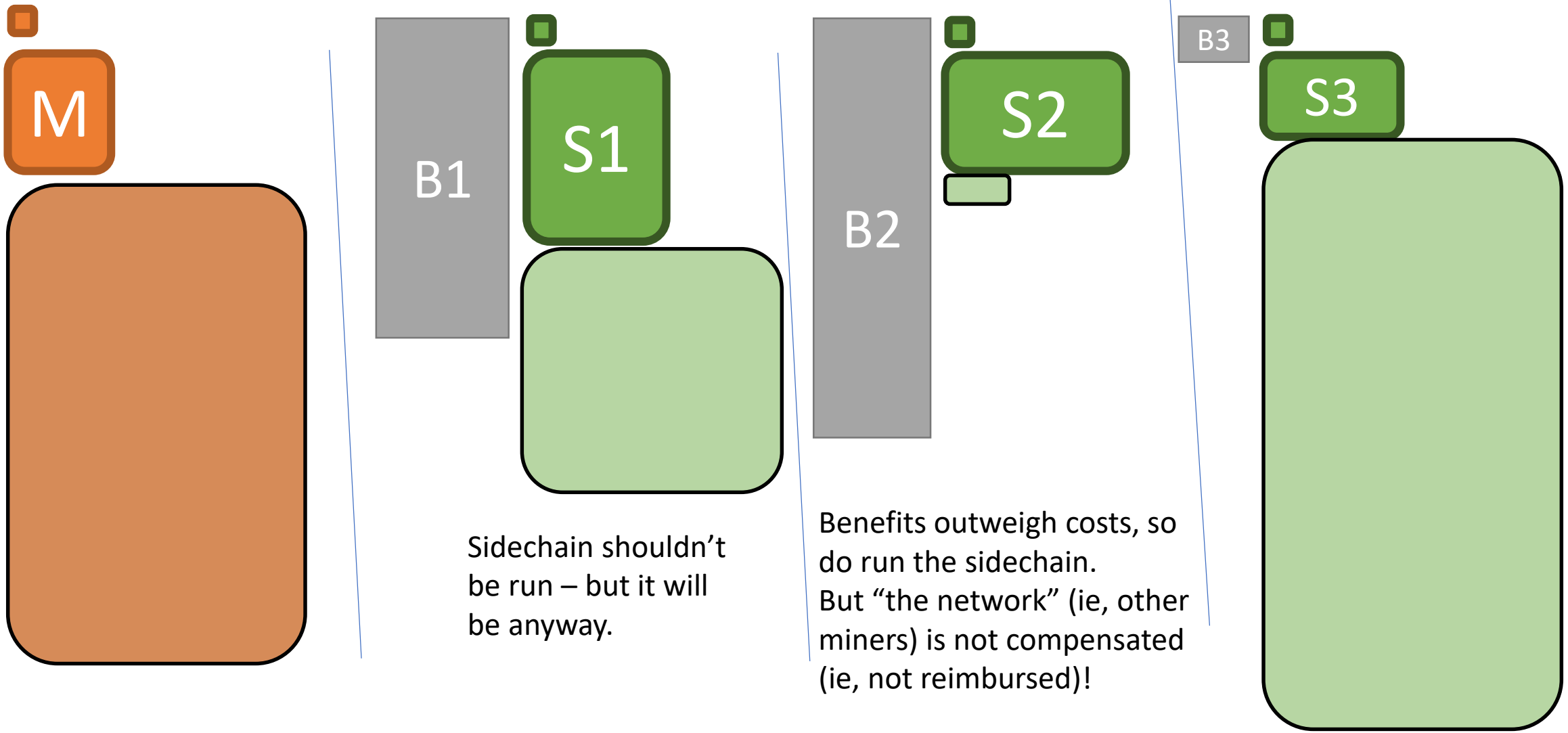
- **Privacy** (Observing Bandwidth)
- Decentralization (Harder to Validate, **fewer seed nodes**)
- Concentration of Power (**Resource Asymmetries** Become More Relevant)

Never

Highly nonlinear and explosive, potentially existential!

Miners may harm other miners.

Miners Imposing On Each Other



Sidechain shouldn't be run – but it will be anyway.

Benefits outweigh costs, so do run the sidechain.
But "the network" (ie, other miners) is not compensated (ie, not reimbursed)!

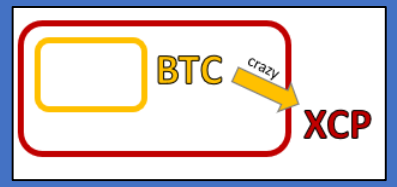
Miner may run this sidechain anyway, relying on pool.

Thus forcing *all* miners to rely on pool, as none can accord externalities.

Blind Merged Mining

Only affects people who run nodes, ie *not* the miners.

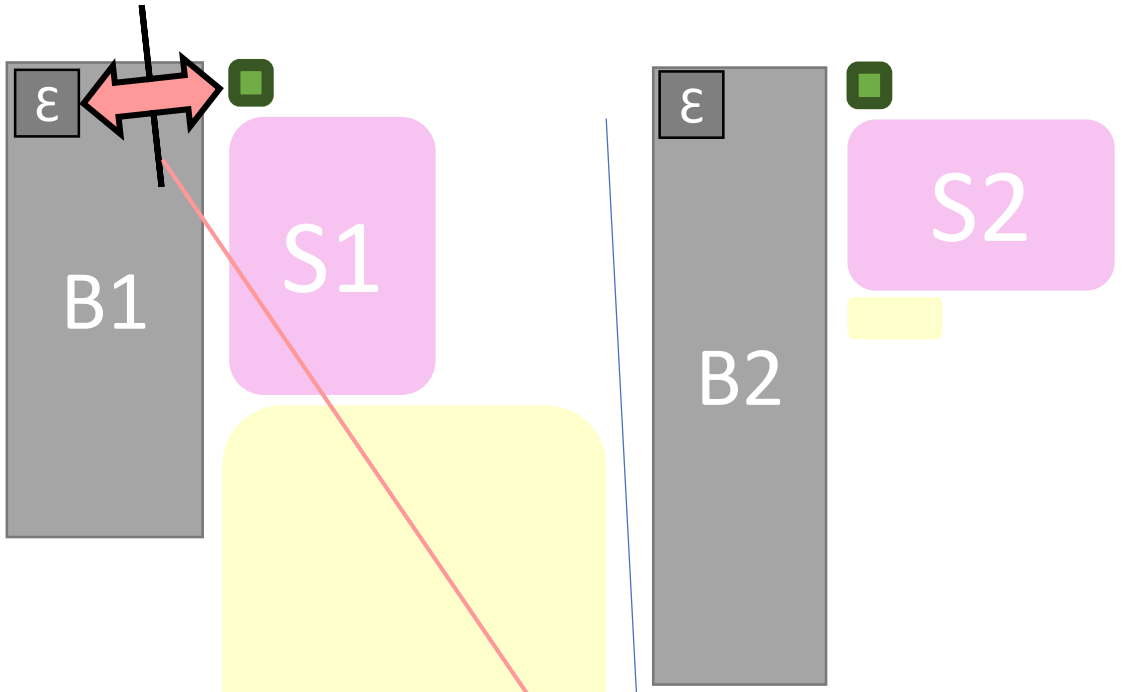
Defined ‘land’ in main:coinbase -- defines the “next mined sidechain header”



OP code letting you ‘buy’ this space.

Basically turns every sidechain full node into a pool administrator.

Gives (100-Ɛ)% fees to hashers, keeps Ɛ for themselves.



Market will drive Ɛ toward zero, probably even lower than the outsourced node validation cost.

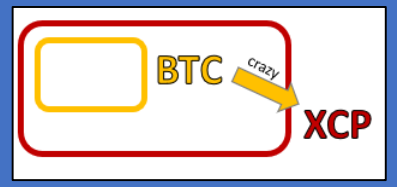
This effectively **equalizes profits**. Miners earn same profit, whether they mine a sidechain or not.

If inter-miner externalities are high, revert to Blind Merged Mining (and don’t pay them).

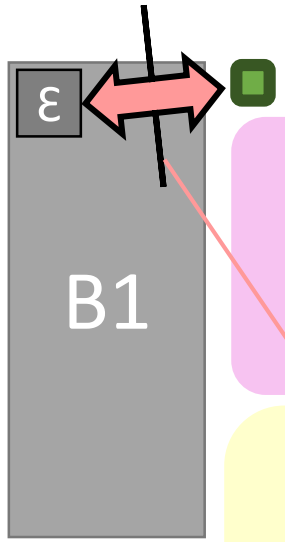
Blind Merged Mining

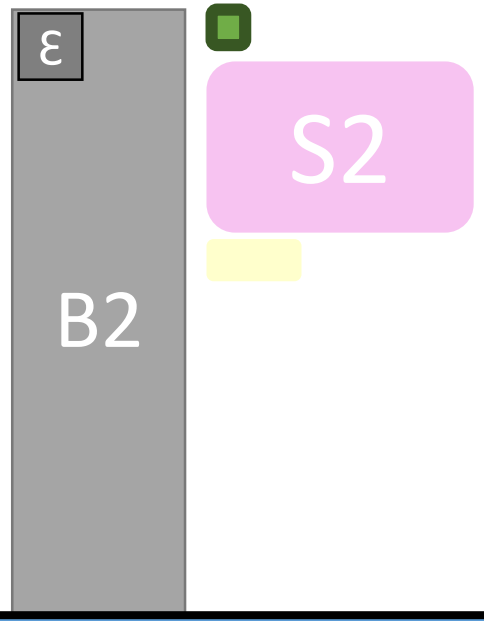
Only affects people who run nodes, ie *not* the miners.

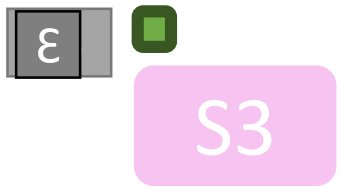
Defined 'land' in main:coinbase -- defines the "next mined sidechain header"



OP code letting you 'buy' this space.







Basic
nod

Massive increase in:

- decentralization,
- pool competitiveness.

Gives (100-S)% fees to hashers, keeps

Pool operators cannot exclude miners.

Market w
probably
outsource

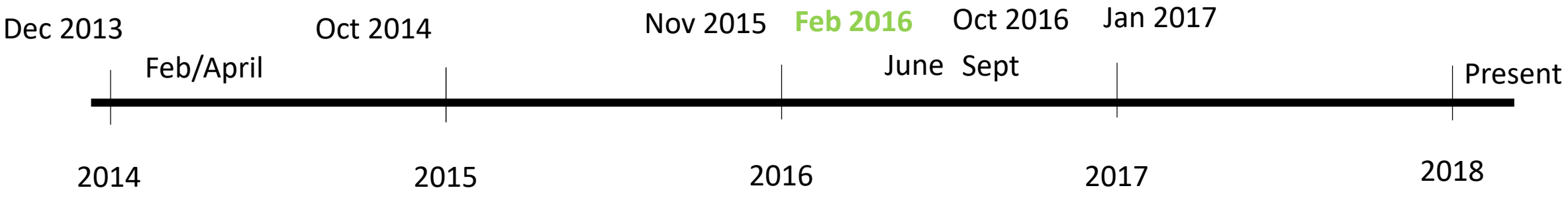
This effect
s ear
they mir

More efficient than regular MM:

- No software upgrade needed (miners don't need to run new, experimental, buggy software.
- Miners are paid in mainchain BTC (as opposed to sidechain coins which they may not want).

h,
nd

Disproportionately Low Support – Misunderstandings?



- Sidechains
  - Very Old ("Drive Chain" much older than SegWit)
  - Solves everyone's problems
  - Has zero drawbacks …
- Suspicious lack of interest.
- Is it **Misunderstandings**?

Helpful Comparisons

Replace “sidechain” with…

1. **“altcoin”** / “counterparty”
   - ecological concerns
   - “sidechain might become too popular”
   - “it would compete with Bitcoin on fees”

2. A **website** (like “Mt Gox”)
   - theft
   - “people might lose their money”
   - This is desirable! – Antifragility! Improvement!
   - *Perfection* neither attainable nor desirable.
   - Difference between DC and other things.

JihanWu-wallet.com

“Safe Imperfection”

Timeline

Progress

//m@-c @mecampbellsoup · 3h

Exactly. Imagine a world in which all the altcoins of today existed as (permission less) $BTC sidechains. I'm sure you have Adam :)

1 2

Giacomo Zucco
@giacomozucco

Following

Replying to @mecampbellsoup @Truthcoin and 17 others

That would be a great world. I think we all agree about that (which btw proves that Paul's theory about "Core", and me, fearing sidechain concept itself because it "kills experts" is just random unsensical bullshit).

9:00 AM - 4 Feb 2018

1 Like

1

belief in the ignorance of experts.

(Richard Feynman)

izquotes.com

"Why Does the Free Market
by Milton
Human Events, 2 Ju
First published in *Farmand*
© Farmand/H

riment, **anti-expert**.

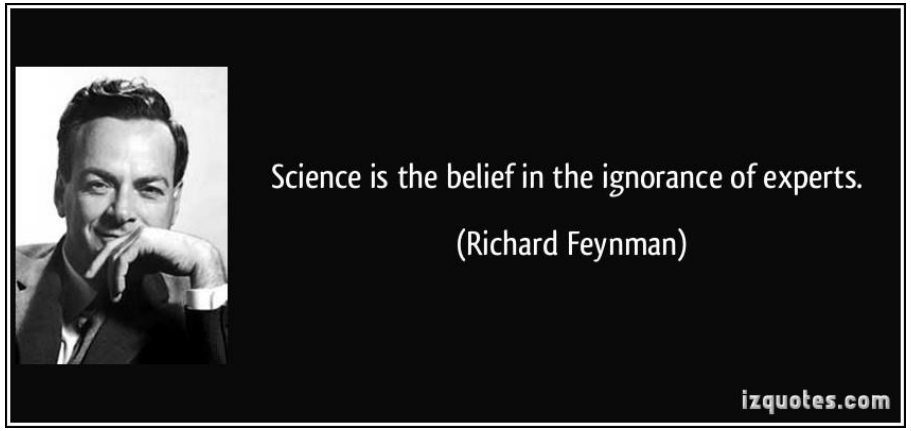
These comm
press, espec
society than
intelligent p
ones who a
to come for
internationa

has such a bad
limited in a free
ked to the able,
ty, they are the
re going to have
g to attend the
society and their

OUR MISSION

Our Lab is the place where we nurture the strongest community of experts in the field hence providing enterprises with the skills to understand and use the blockchain technology.

Progress vs Expertise



"Why Does the Free Market Have Such a Bad Press?"
by Milton Friedman
Human Events, 2 July 1966, pp. 8, 14
First published in *Farmand* (Oslo), 12 February 1966
© Farmand/Human Events

Drivechain is pro-experiment, **anti-expert**.

These comments suggest the final reason I want to mention why free enterprise has such a bad press, especially among intellectuals. The role of the intellectual is much more limited in a free society than it is in a controlled society. I was most impressed with this as I talked to the able, intelligent people at the University of Malaysia. In a planned, collectivist society, they are the ones who are going to sit in the seats of power and to whom the businessmen are going to have to come for import permits, licenses and so on. They are the ones who are going to attend the international conferences and meetings. Let Malaysia follow the path of a free society and their role will be very different. The minority Chinese in Malaysia are the most effective and energetic businessmen and hence will be in the positions of power in a free market society. The intellectuals will be reduced to being their advisers or simply teachers in a university. Of course, no intellectual will say this explicitly, but implicitly he knows well that he can run the country better than "they" can.

Conclusion

- Goals
  - Defeat Altcoin Competition, permanently
  - Resolve Scalability Conflict ("win-win"), permanently.
  - Resolve questions of *governance*. Experiments can be tried safely on opt-in basis.
- Status
  - Code v0.1 is **finished**!!
  - Recently rebased to latest Bitcoin Core.
- Help Needed
  - Code Review – Unclear Review Incentives
  - *Issues* are open on GitHub.

Thanks CryptAxe

Thanks Ben Goldhaber