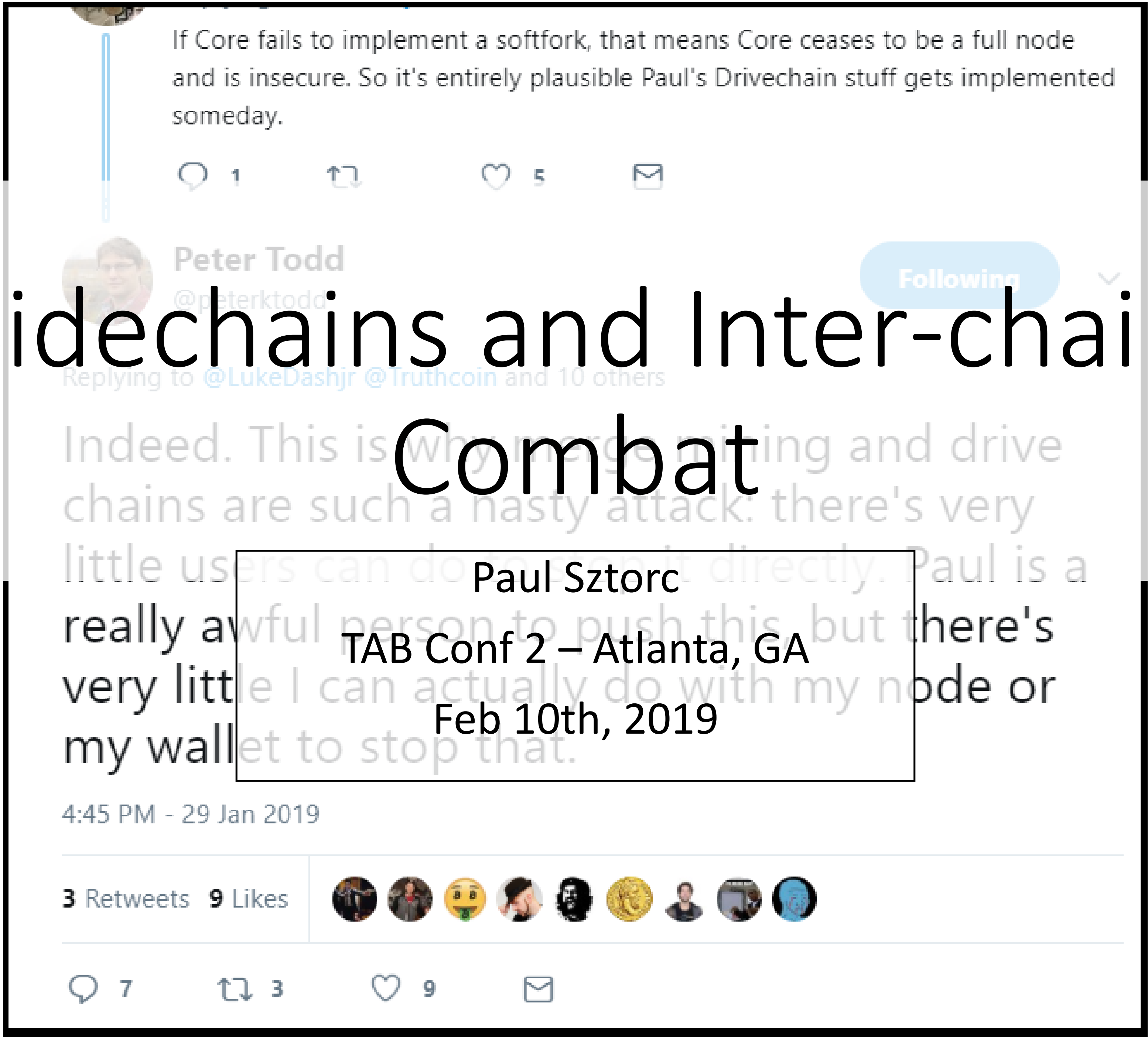
Sidechains and Inter-chain Combat

Paul Sztorc

TAB Conf 2 – Atlanta, GA

Feb 10th, 2019



If Core fails to implement a softfork, that means Core ceases to be a full node and is insecure. So it's entirely plausible Paul's Drivechain stuff gets implemented someday.

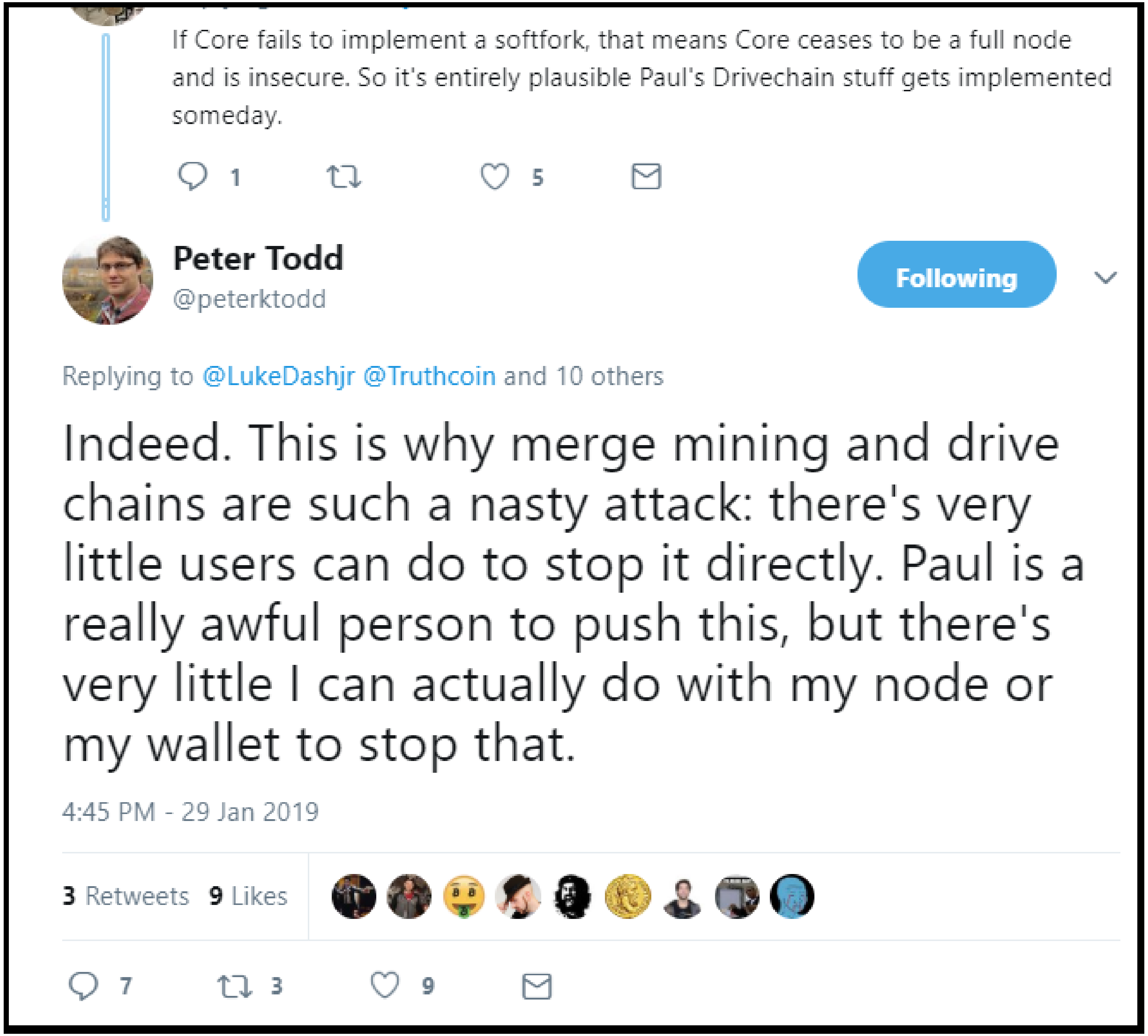
Peter Todd
@peterktodd

Replying to @LukeDashjr @Truthcoin and 10 others

Indeed. This is why merge mining and drive chains are such a nasty attack: there's very little users can do to stop it directly. Paul is a really awful person to push this, but there's very little I can actually do with my node or my wallet to stop that.

4:45 PM - 29 Jan 2019

3 Retweets 9 Likes



If Core fails to implement a softfork, that means Core ceases to be a full node and is insecure. So it's entirely plausible Paul's Drivechain stuff gets implemented someday.

1 5

Peter Todd
@peterktodd

Replying to @LukeDashjr @Truthcoin and 10 others

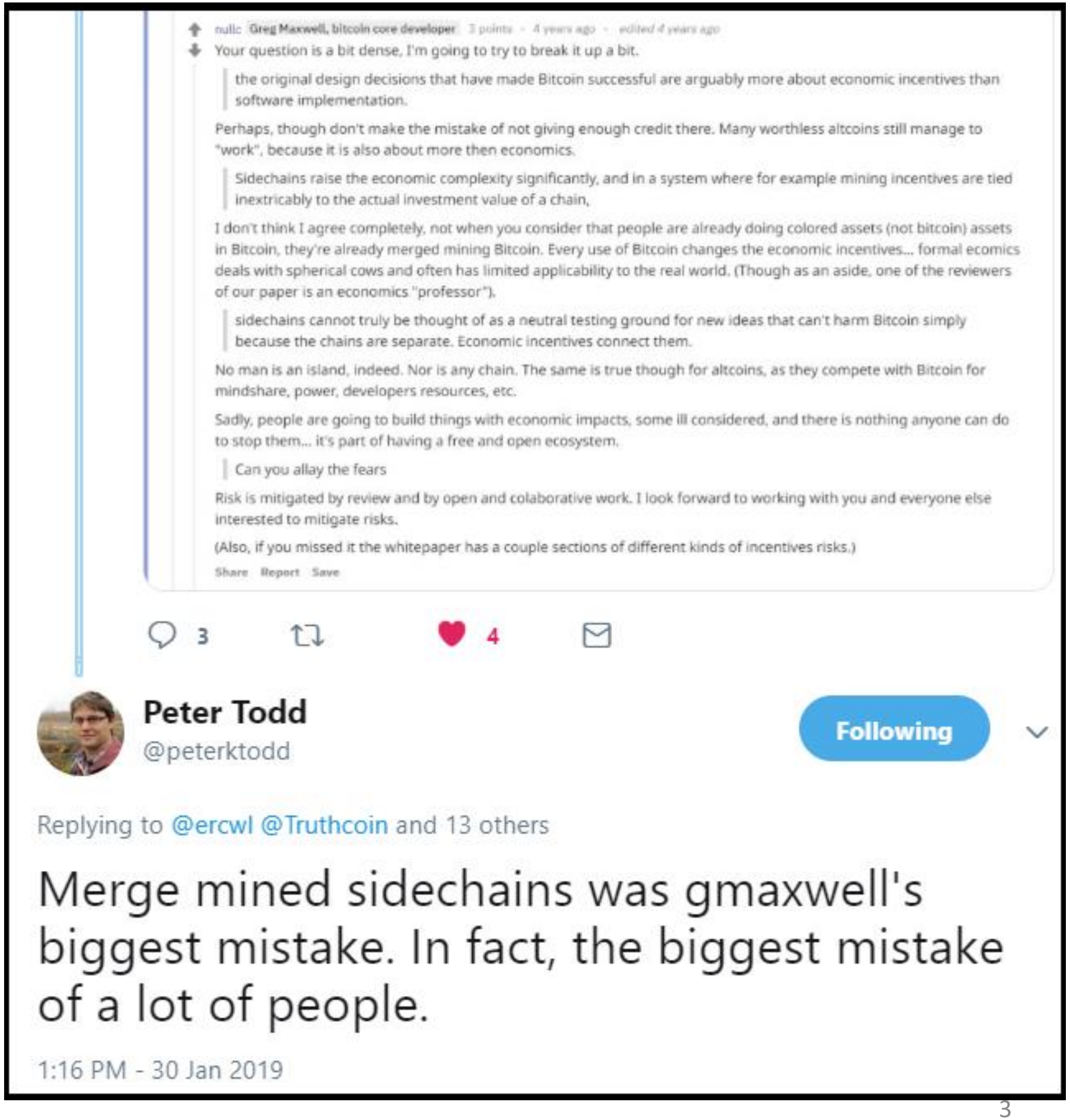
Indeed. This is why merge mining and drive chains are such a nasty attack: there's very little users can do to stop it directly. Paul is a really awful person to push this, but there's very little I can actually do with my node or my wallet to stop that.

4:45 PM - 29 Jan 2019

3 Retweets 9 Likes

7 3 9

Gmaxwell's Biggest Mistake



nullc Greg Maxwell, bitcoin core developer 3 points · 4 years ago · edited 4 years ago

Your question is a bit dense, I'm going to try to break it up a bit.

> the original design decisions that have made Bitcoin successful are arguably more about economic incentives than software implementation.

Perhaps, though don't make the mistake of not giving enough credit there. Many worthless altcoins still manage to "work", because it is also about more then economics.

> Sidechains raise the economic complexity significantly, and in a system where for example mining incentives are tied inextricably to the actual investment value of a chain,

I don't think I agree completely, not when you consider that people are already doing colored assets (not bitcoin) assets in Bitcoin, they're already merged mining Bitcoin. Every use of Bitcoin changes the economic incentives... formal ecomics deals with spherical cows and often has limited applicability to the real world. (Though as an aside, one of the reviewers of our paper is an economics "professor").

> sidechains cannot truly be thought of as a neutral testing ground for new ideas that can't harm Bitcoin simply because the chains are separate. Economic incentives connect them.

No man is an island, indeed. Nor is any chain. The same is true though for altcoins, as they compete with Bitcoin for mindshare, power, developers resources, etc.

Sadly, people are going to build things with economic impacts, some ill considered, and there is nothing anyone can do to stop them... it's part of having a free and open ecosystem.

> Can you allay the fears

Risk is mitigated by review and by open and colaborative work. I look forward to working with you and everyone else interested to mitigate risks.

(Also, if you missed it the whitepaper has a couple sections of different kinds of incentives risks.)

Peter Todd
@peterktodd

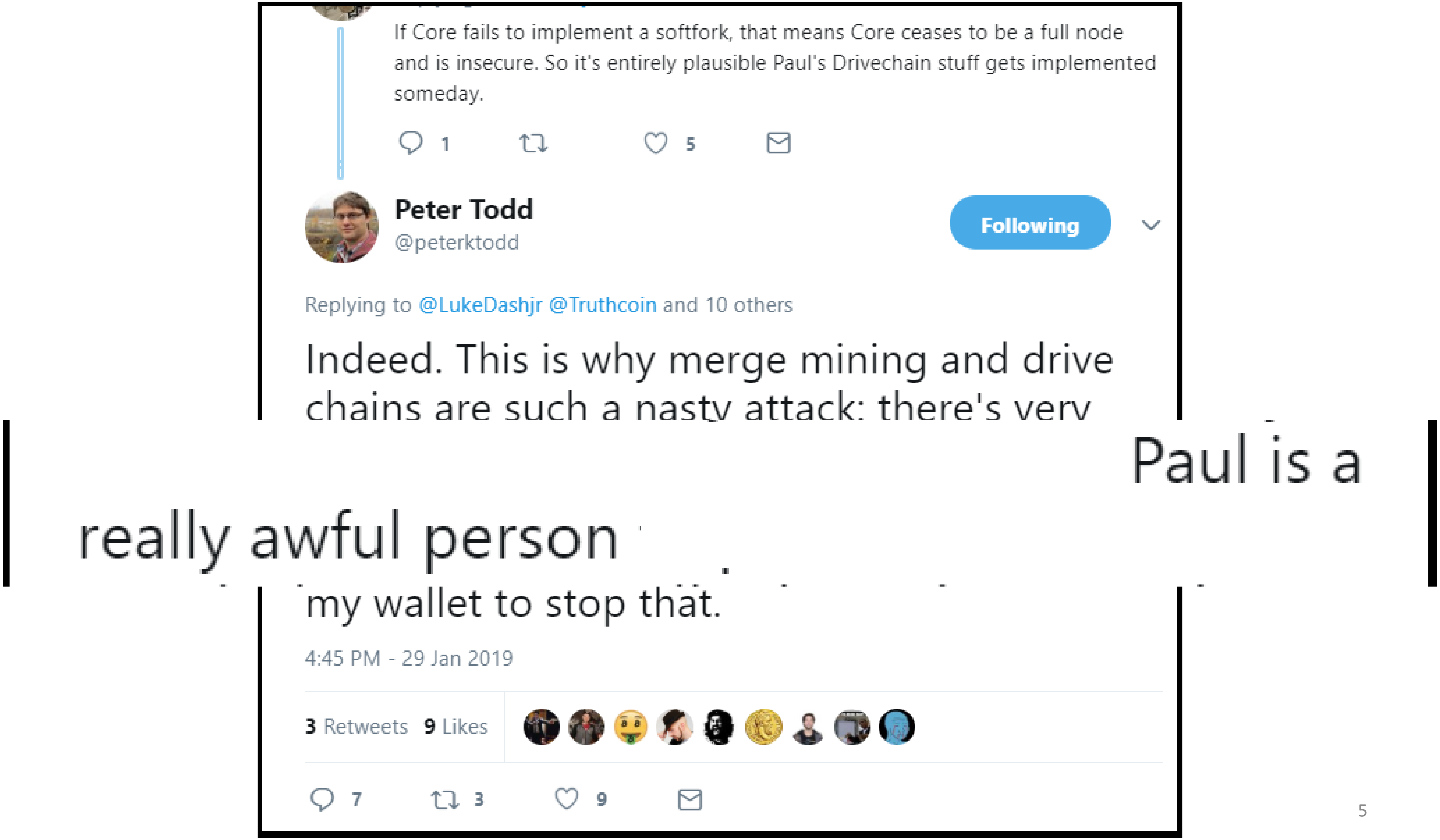
Replying to @ercwl @Truthcoin and 13 others

Merge mined sidechains was gmaxwell's biggest mistake. In fact, the biggest mistake of a lot of people.

1:16 PM - 30 Jan 2019

Who Am I?

- Pre-Bitcoin
  - BA Economics, Psychology; Mathematics, MS-M OR, MBA Finance
  - Financial Consulting -- Healthcare IT
  - Statistician Yale Econ Dept – Bill Nordhaus (2018 Nobel)
- Roger Ver – Truthcoin / Hivemind
  - Bloq early 2016 – Drivechain ; current affiliation: Tierion
- Truthcoin.info Blog
  - “Nothing is Cheaper than Proof of Work” (Nov 2014, Aug 2015)
  - “Private Blockchains, Demystified” (Nov 2014, Mar 2016)
  - “Measuring Decentralization” (Sep 2015)
  - “Fork Futures” (Jul 2015, Oct 2017)
  - “Drivechain: The Simple Two-way peg” (Nov 2015)
- ‘Scaling Bitcoin’ 1-3 (Presenter); Scaling 4 (Program Committee)



If Core fails to implement a softfork, that means Core ceases to be a full node and is insecure. So it's entirely plausible Paul's Drivechain stuff gets implemented someday.

Peter Todd
@peterktodd

Replying to @LukeDashjr @Truthcoin and 10 others

Indeed. This is why merge mining and drive chains are such a nasty attack: there's very

Paul is a really awful person

my wallet to stop that.

4:45 PM - 29 Jan 2019

3 Retweets **9** Likes

Timeline

Like 6 months ago

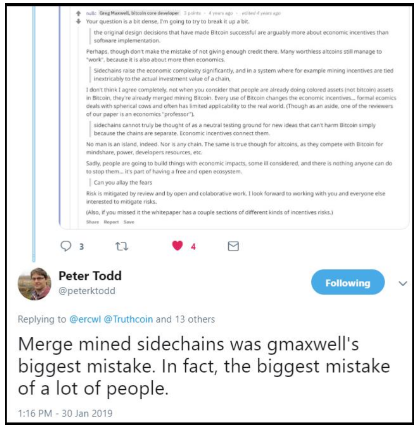
Agree to give talk.

December

Interchain combat.

Choose topic.

Jan 30th



nullc Greg Maxwell, bitcoin core developer 3 points · 4 years ago · edited 4 years ago

Your question is a bit dense, I'm going to try to break it up a bit.

> the original design decisions that have made Bitcoin successful are arguably more about economic incentives than software implementation.

Perhaps, though don't make the mistake of not giving enough credit there. Many worthless altcoins still manage to "work", because it is also about more then economics.

> Sidechains raise the economic complexity significantly, and in a system where for example mining incentives are tied inextricably to the actual investment value of a chain,

I don't think I agree completely, not when you consider that people are already doing colored assets (not bitcoin) assets in Bitcoin, they're already merged mining Bitcoin. Every use of Bitcoin changes the economic incentives... formal ecomics deals with spherical cows and often has limited applicability to the real world. (Though as an aside, one of the reviewers of our paper is an economics "professor").

> sidechains cannot truly be thought of as a neutral testing ground for new ideas that can't harm Bitcoin simply because the chains are separate. Economic incentives connect them.

No man is an island, indeed. Nor is any chain. The same is true though for altcoins, as they compete with Bitcoin for mindshare, power, developers resources, etc.

Sadly, people are going to build things with economic impacts, some ill considered, and there is nothing anyone can do to stop them... it's part of having a free and open ecosystem.

> Can you allay the fears

Risk is mitigated by review and by open and colaborative work. I look forward to working with you and everyone else interested to mitigate risks.

(Also, if you missed it the whitepaper has a couple sections of different kinds of incentives risks.)

Peter Todd
@peterktodd

Replying to @ercwl @Truthcoin and 13 others

Merge mined sidechains was gmaxwell's biggest mistake. In fact, the biggest mistake of a lot of people.

1:16 PM - 30 Jan 2019

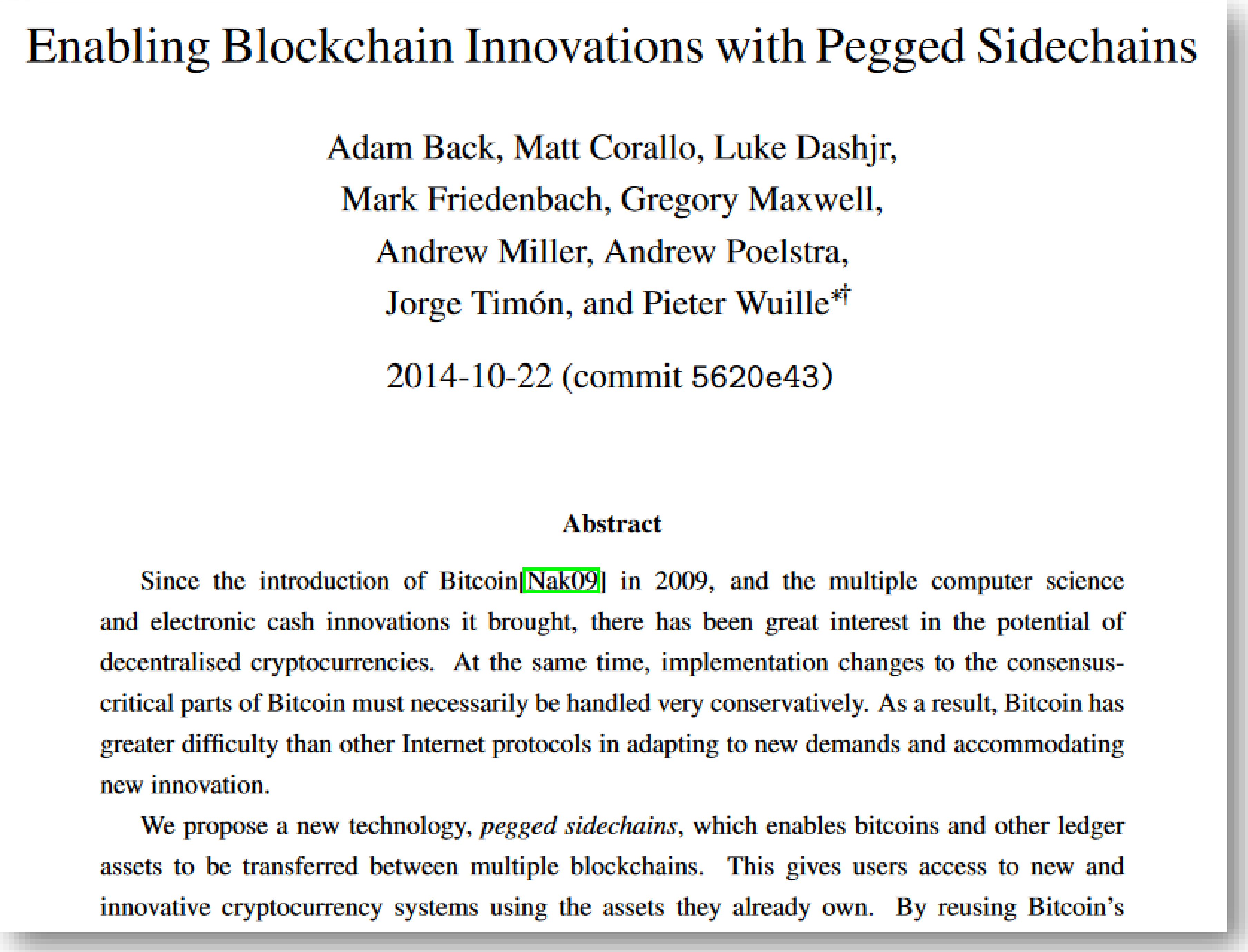
Cryptotwitter intrigue.

Feb 10th

Today

Agenda

1. Sidechains: Universal Altcoin Simulation (and Compression)
2. How it works
3. Critiques of Sidechains
4. Sidechain Privatization (“Interchain combat” and “flipped work”).
   - Name-leeching.
   - Oracle reputation-leeching.
   - Fee-leeching.



Enabling Blockchain Innovations with Pegged Sidechains

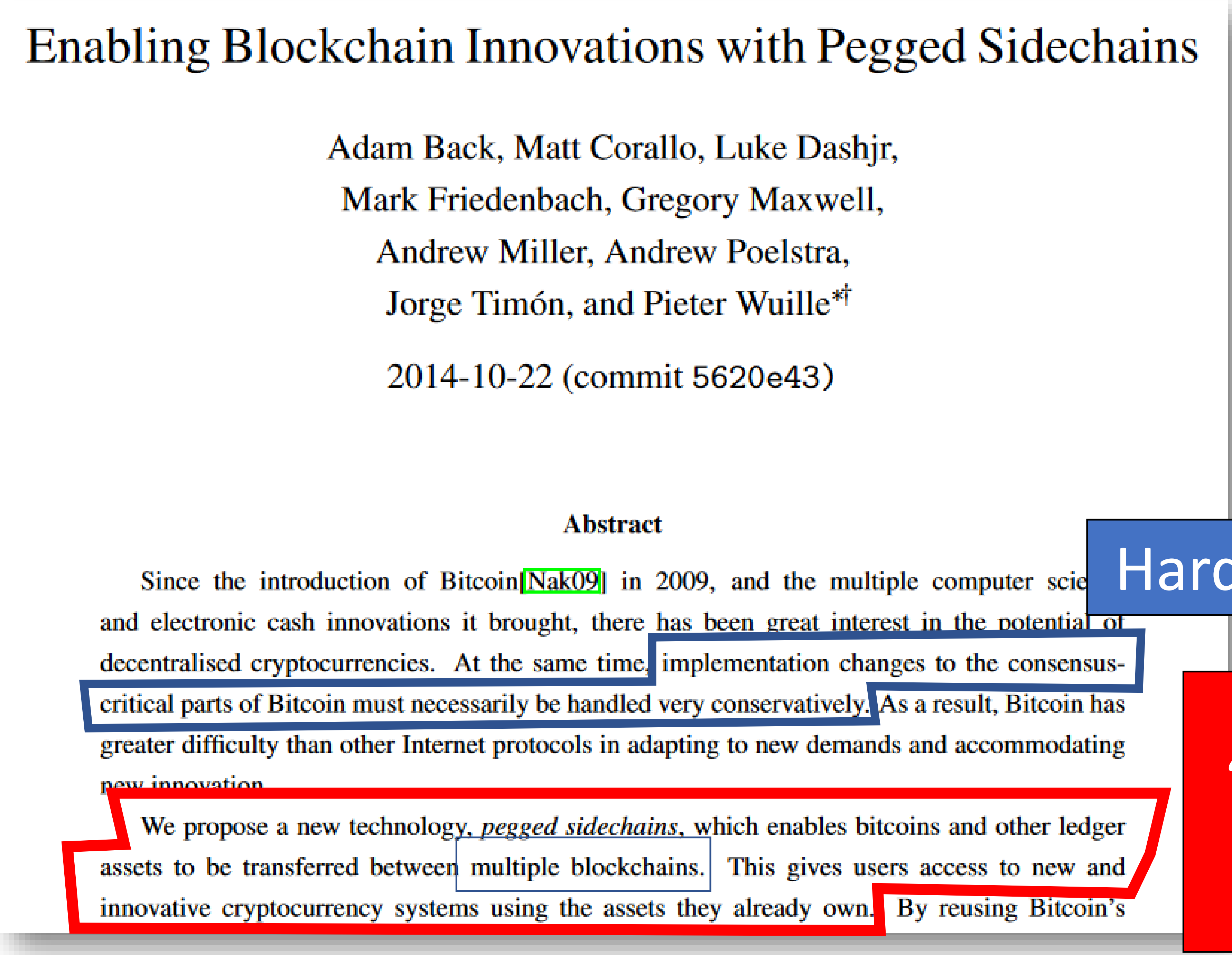
Adam Back, Matt Corallo, Luke Dashjr,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille*†

2014-10-22 (commit 5620e43)

Abstract

Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer science and electronic cash innovations it brought, there has been great interest in the potential of decentralised cryptocurrencies. At the same time, implementation changes to the consensus-critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin's



Enabling Blockchain Innovations with Pegged Sidechains

Adam Back, Matt Corallo, Luke Dashjr,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille*†

2014-10-22 (commit 5620e43)

Abstract

Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer scie and electronic cash innovations it brought, there has been great interest in the potential of decentralised cryptocurrencies. At the same time, implementation changes to the consensus-critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin’s

Hard forks bad

Opt-in “compart-ments” good

1 person clipped this slide

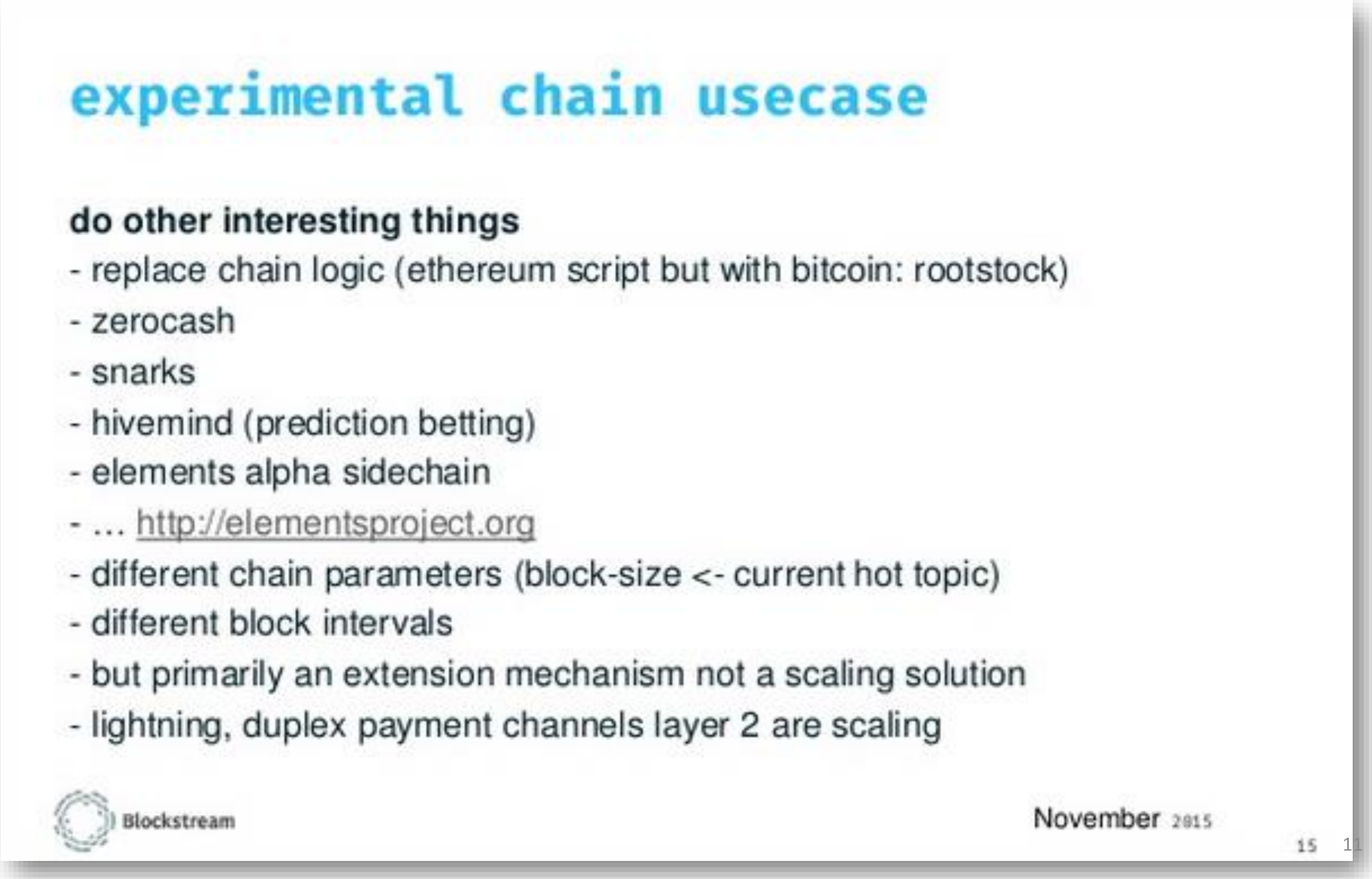
Blockstream

Sidechains: weaving a network of blockchains with Bitcoin

Hive event

February 17, 2016

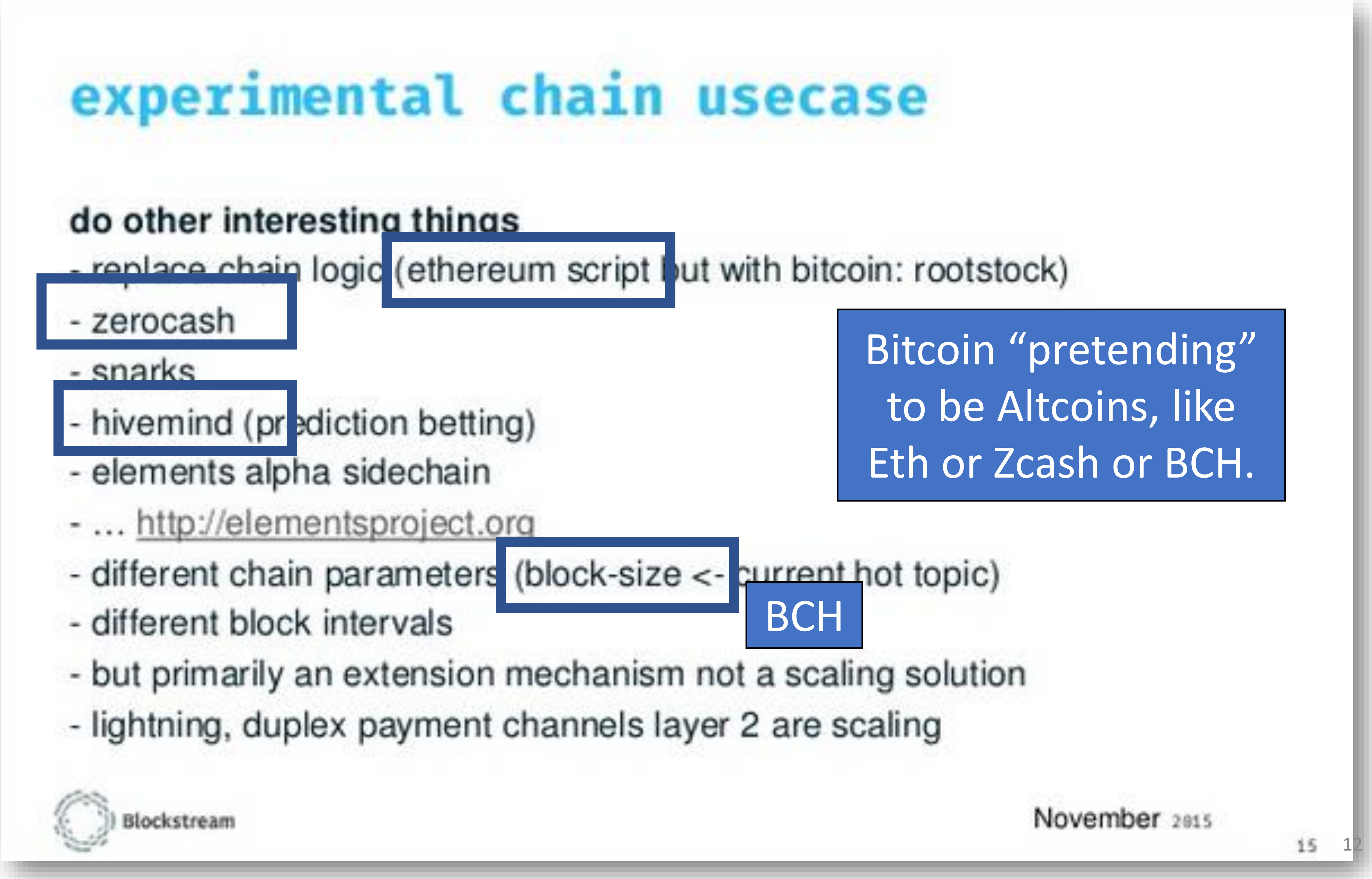
Adam Back, PhD



experimental chain usecase

do other interesting things

- replace chain logic (ethereum script but with bitcoin: rootstock)
- zerocash
- snarks
- hivemind (prediction betting)
- elements alpha sidechain
- … http://elementsproject.org
- different chain parameters (block-size <- current hot topic)
- different block intervals
- but primarily an extension mechanism not a scaling solution
- lightning, duplex payment channels layer 2 are scaling



experimental chain usecase

do other interesting things

- replace chain logic (ethereum script but with bitcoin: rootstock)
- zerocash
- sparks
- hivemind (prediction betting)
- elements alpha sidechain
- … http://elementsproject.org
- different chain parameters (block-size <- current hot topic)
- different block intervals
- but primarily an extension mechanism not a scaling solution
- lightning, duplex payment channels layer 2 are scaling

Blockstream

November 2015

15

Bitcoin “pretending” to be Altcoins, like Eth or Zcash or BCH.

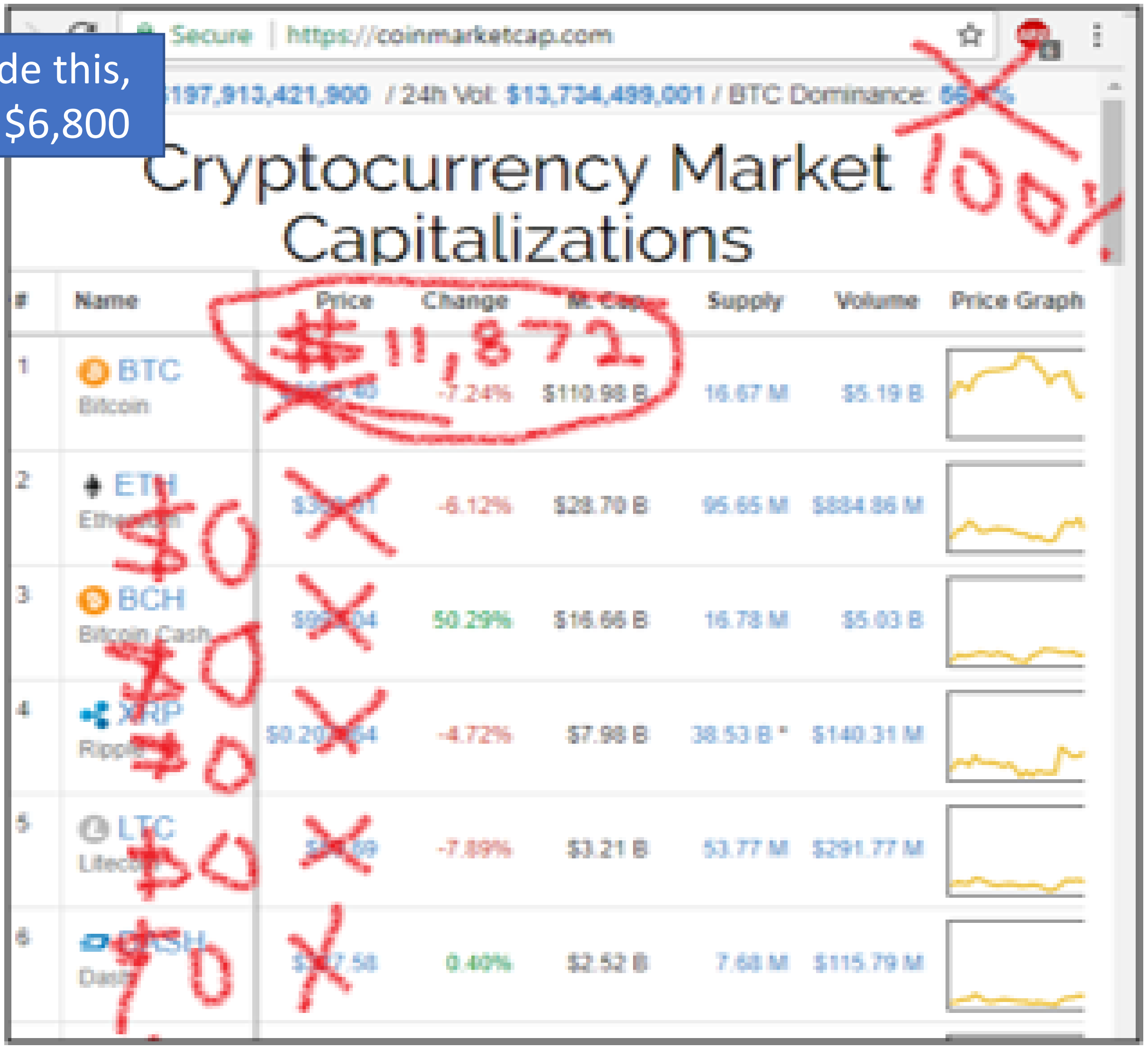
BCH

My definition: universal altcoin simulator.

Iterative Deletion

Popularity → location, not price

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

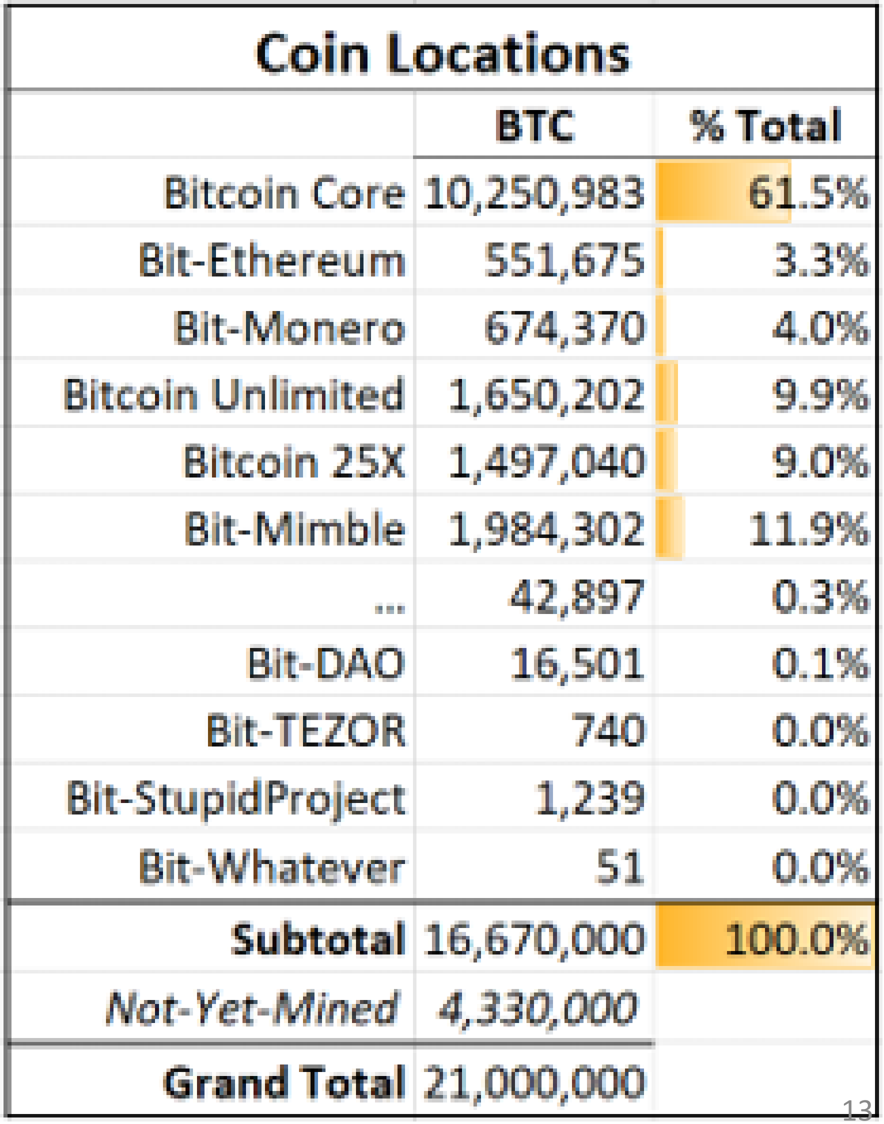


Secure | https://coinmarketcap.com

$197,913,421,900 / 24h Vol: $13,734,499,001 / BTC Dominance: ~~56.[illegible]%~~ 100%

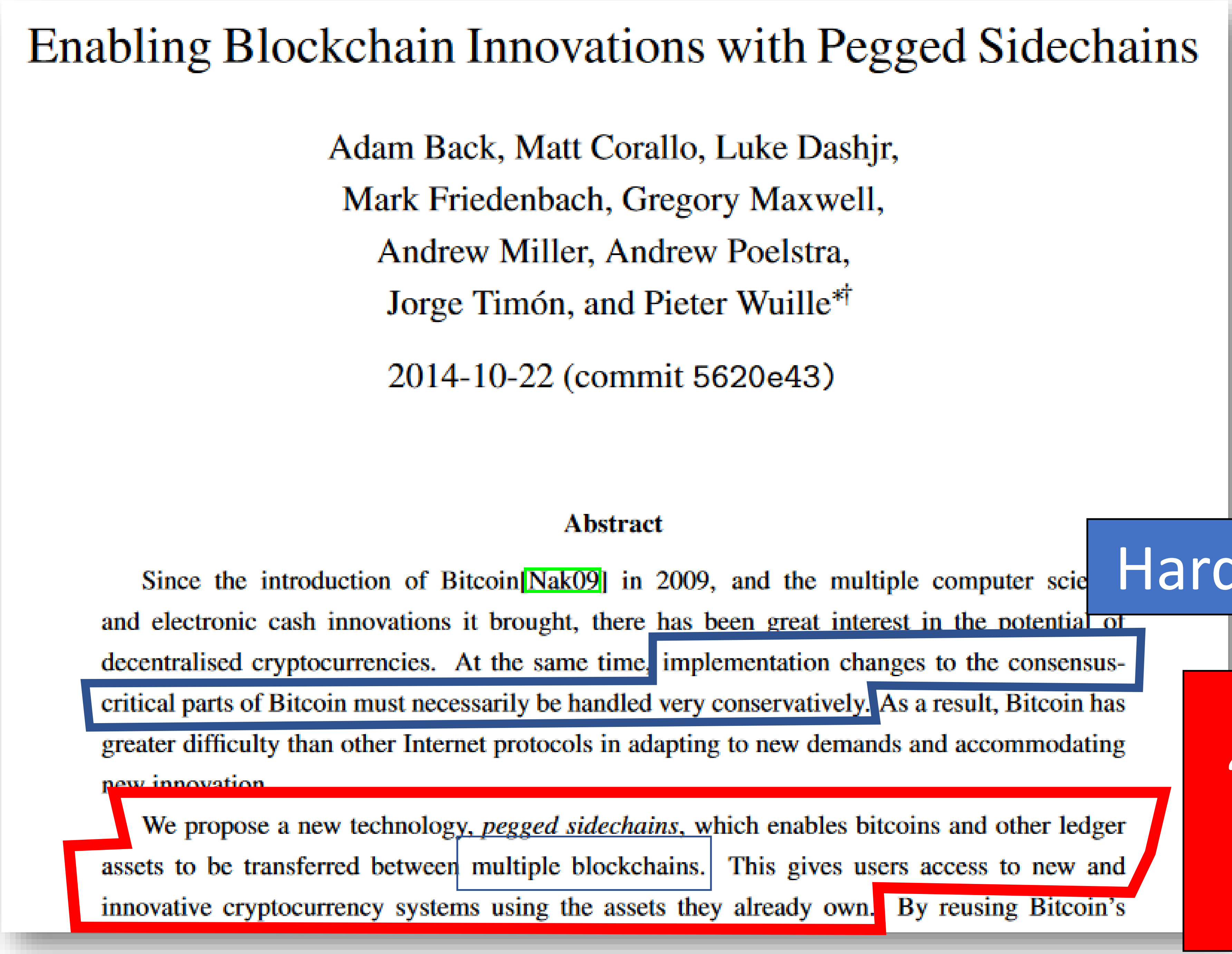
Cryptocurrency Market Capitalizations

#	Name	Price	Change	Mkt Cap	Supply	Volume	Price Graph
1	BTC Bitcoin	~~[illegible].40~~ $11,872	-7.24%	$110.98 B	16.67 M	$5.19 B	
2	ETH Ethereum $0	~~[illegible]~~	-6.12%	$28.70 B	95.65 M	$884.86 M	
3	BCH Bitcoin Cash $0	~~$9[illegible]04~~	50.29%	$16.66 B	16.78 M	$5.03 B	
4	XRP Ripple $0	~~$0.20[illegible]64~~	-4.72%	$7.98 B	38.53 B *	$140.31 M	
5	LTC Litecoin $0	~~[illegible]69~~	-7.89%	$3.21 B	53.77 M	$291.77 M	
6	DASH Dash $0	~~$[illegible]7.58~~	0.40%	$2.52 B	7.68 M	$115.79 M	



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 25X	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	



Enabling Blockchain Innovations with Pegged Sidechains

Adam Back, Matt Corallo, Luke Dashjr,
Mark Friedenbach, Gregory Maxwell,
Andrew Miller, Andrew Poelstra,
Jorge Timón, and Pieter Wuille*†

2014-10-22 (commit 5620e43)

Abstract

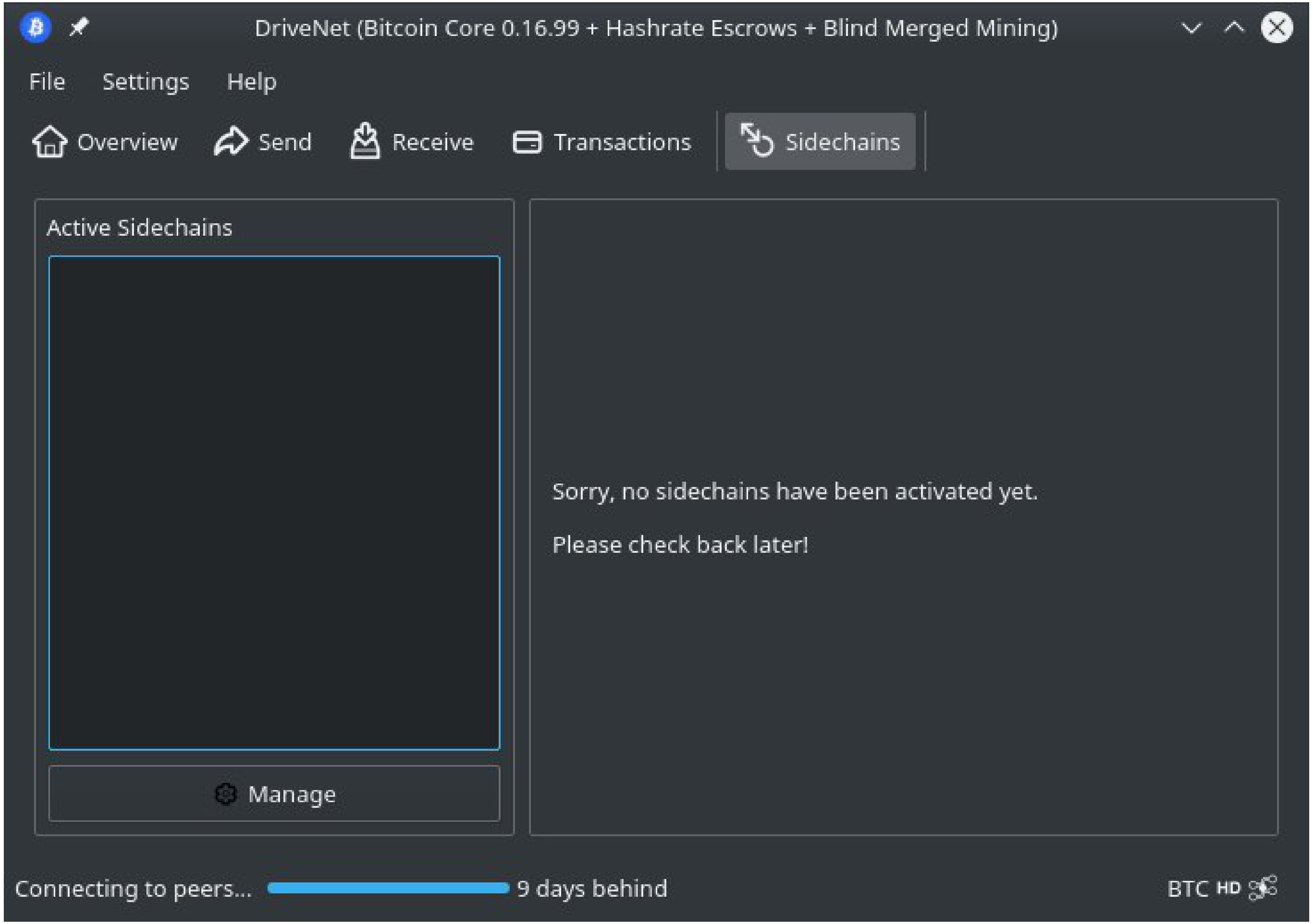
Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer scie and electronic cash innovations it brought, there has been great interest in the potential of decentralised cryptocurrencies. At the same time, implementation changes to the consensus-critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation.

We propose a new technology, *pegged sidechains*, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin's

Hard forks bad

Opt-in "compart-ments" good.

We Built It

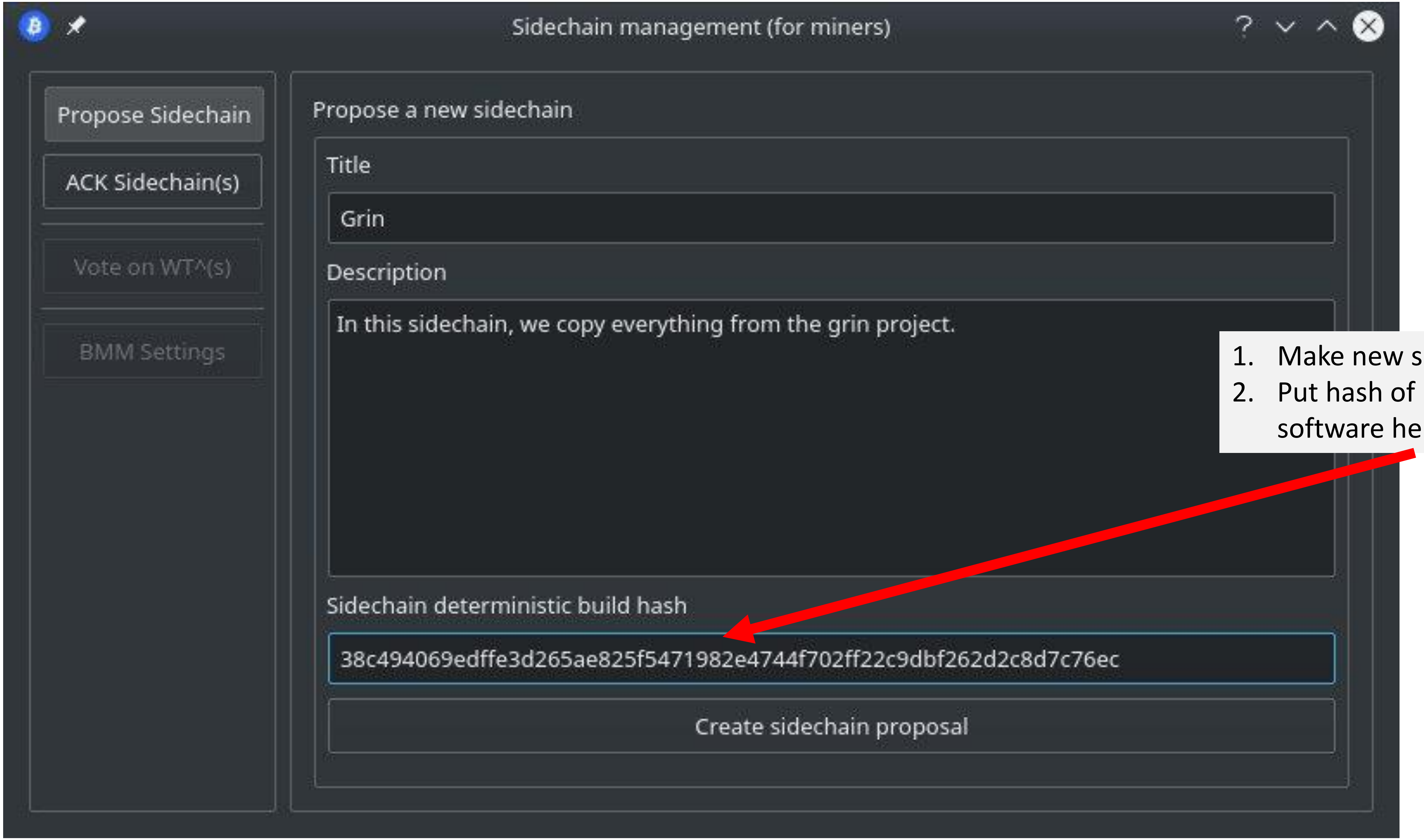


DriveNet (Bitcoin Core 0.16.99 + Hashrate Escrows + Blind Merged Mining)

Sorry, no sidechains have been activated yet.

Please check back later!

Connecting to peers... 9 days behind



Propose a new sidechain

Title

Grin

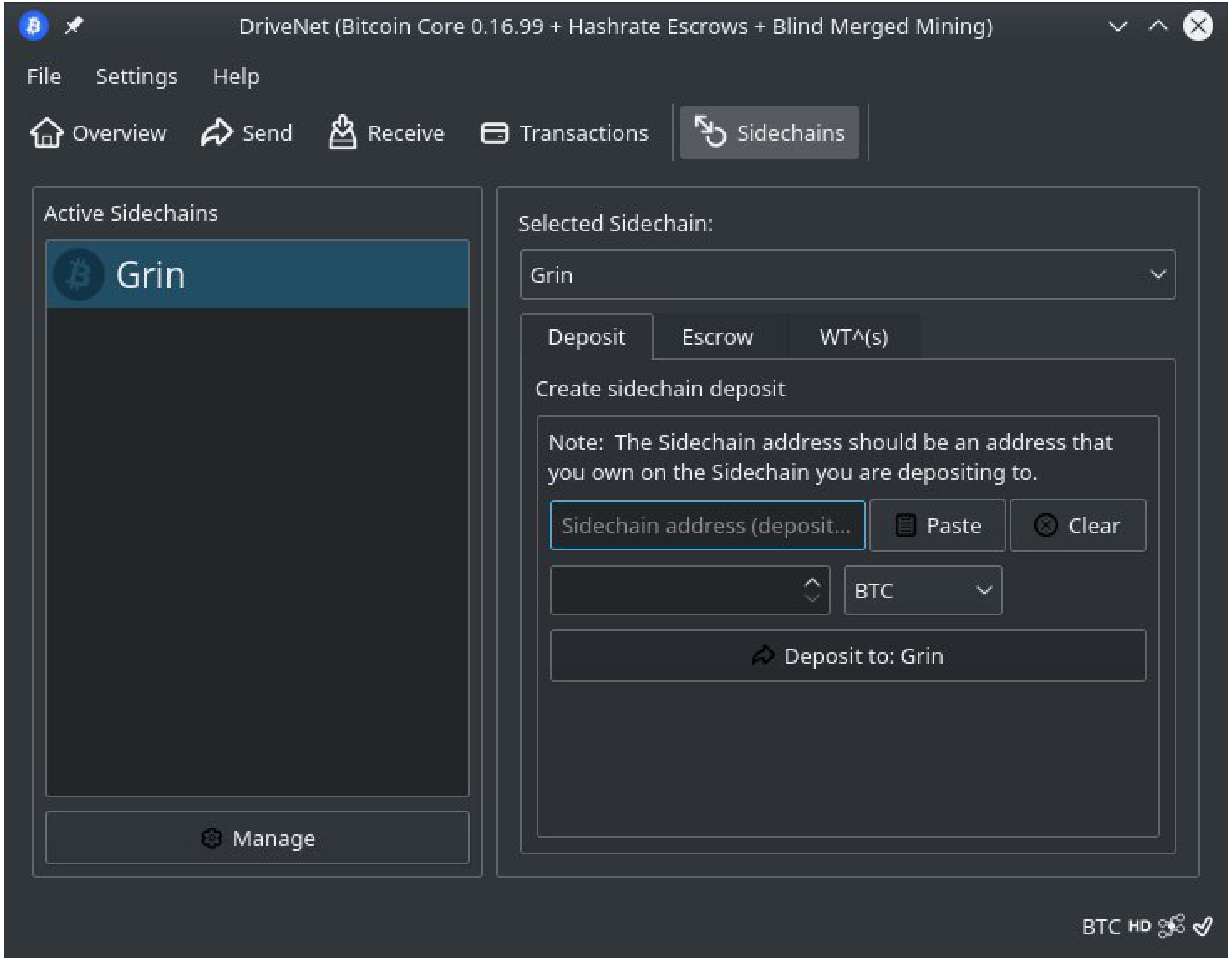
Description

In this sidechain, we copy everything from the grin project.

Sidechain deterministic build hash

38c494069edffe3d265ae825f5471982e4744f702ff22c9dbf262d2c8d7c76ec

1. Make new software.
2. Put hash of new software here.



DriveNet (Bitcoin Core 0.16.99 + Hashrate Escrows + Blind Merged Mining)

Selected Sidechain: Grin

Create sidechain deposit

Note: The Sidechain address should be an address that you own on the Sidechain you are depositing to.

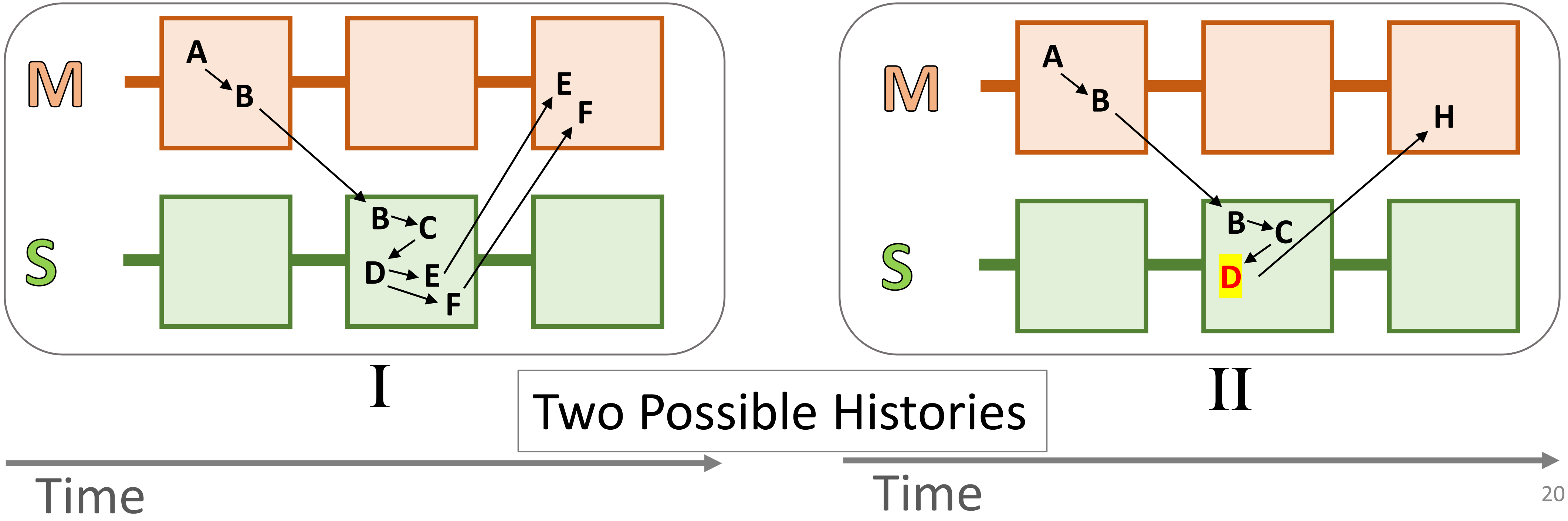
How does it work?

Two pieces

1. **Hashrate Escrow** -- A "Container UTXO" that *compresses* 3-6 months of sidechain data into a fixed 32-bytes.
2. **Blind Merged Mining** -- Replaces the act of running a sidechain node with the act of including a single high-fee transaction.

Sidechain Compression

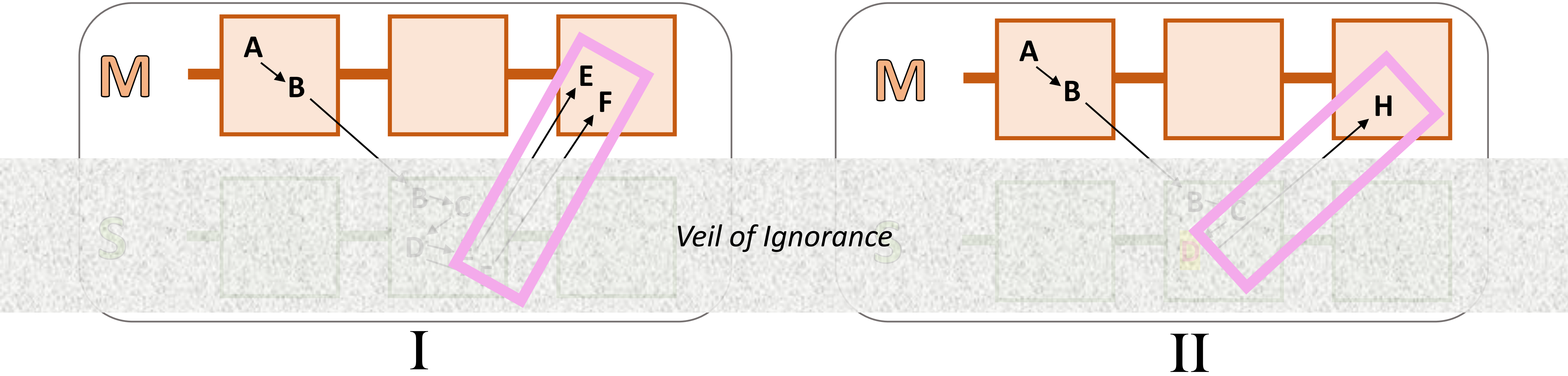
- Mainchain full nodes do not validate sidechain's rules/data.
- But, then, an *invalid withdrawal* must be treated **exactly the same** as a valid one! There is no basis for discriminating between them.



Two Possible Histories

Sidechain Compression

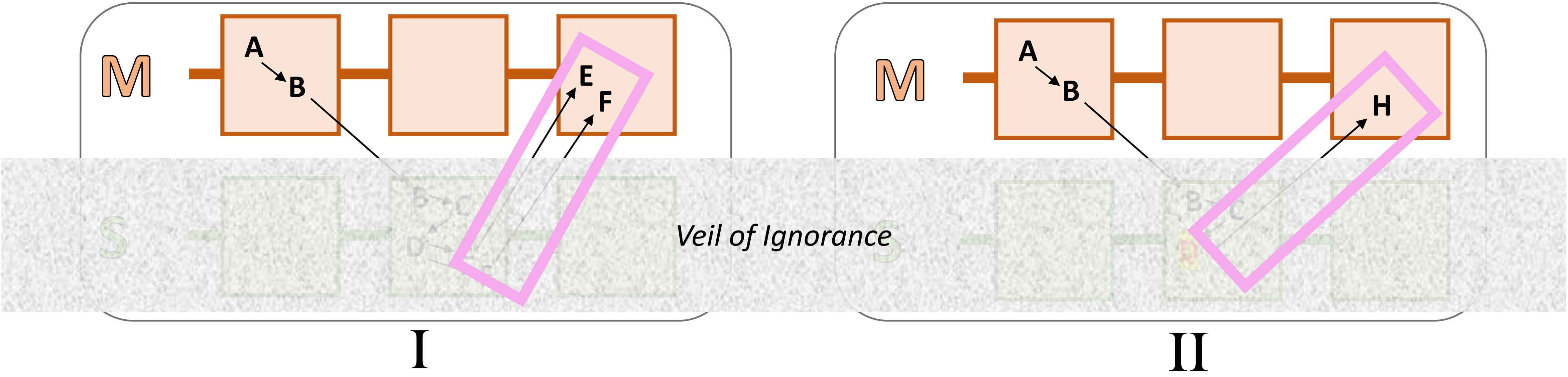
- Mainchain full nodes do not validate sidechain's rules/data.
- But, then, an ***invalid withdrawal*** must be treated **exactly the same** as a valid one! There is no basis for discriminating between them.



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

Sidechain Compression

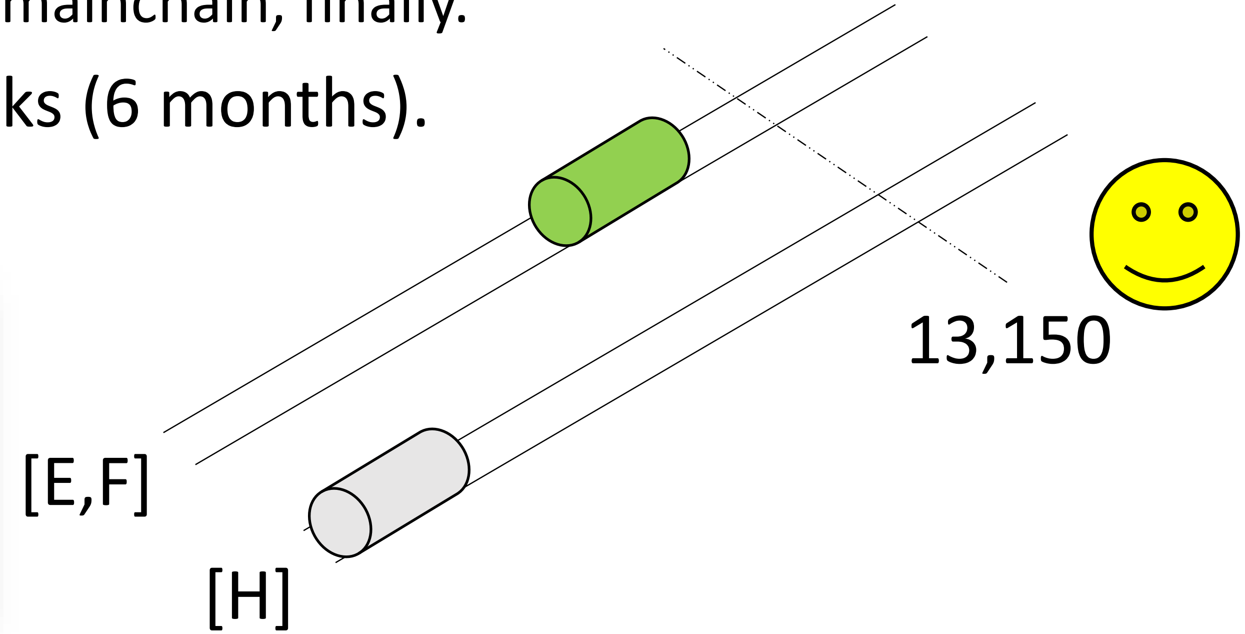
- 32-bytes per 3-6 months.
- We *just assume* that the bytes are correct.
- Sidechain full/SPV nodes are both yelling these bytes as loud as they can.

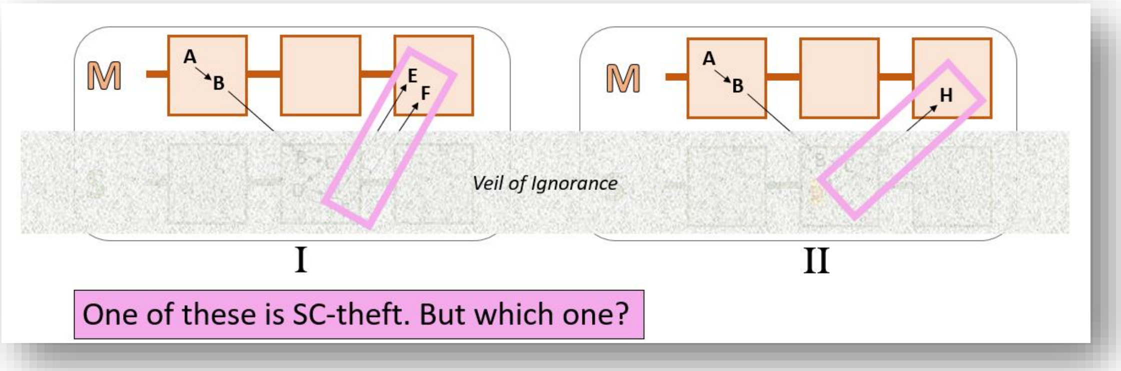


One of these is SC-theft. But which one?

[E,F] vs [H] – Traincar metaphor.

- If a traincar advances 13,150 places (3 months worth of confirmations), it crosses the ‘**finish line**’. Its txns can be included in a main:block.
  - “Passengers” can “disembark”.
  - BTC has moved from sidechain to mainchain, finally.
- Trains “expire” after 26,300 blocks (6 months).

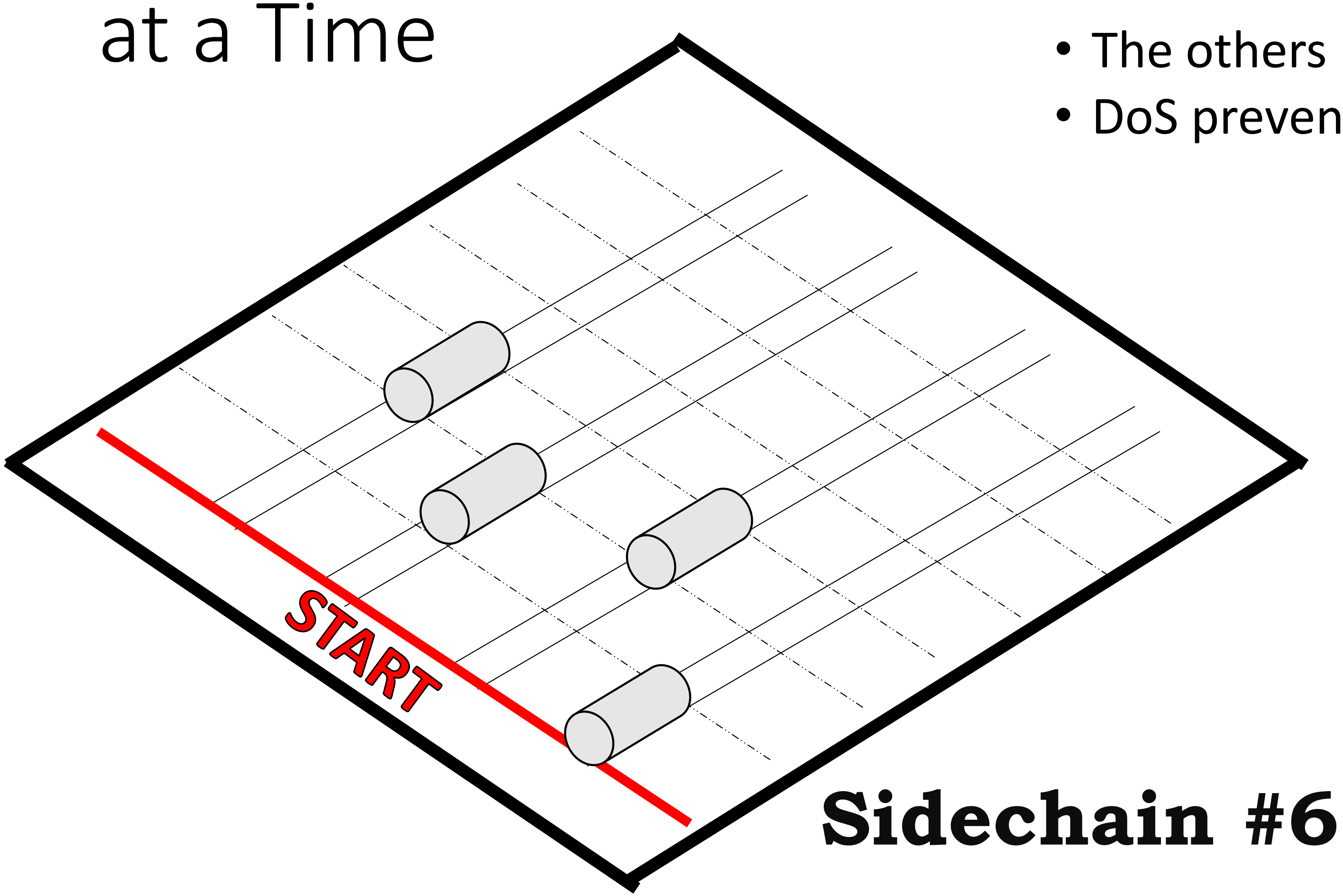




One of these is SC-theft. But which one?

Per Sidechain, Only One Traincar can advance at a Time

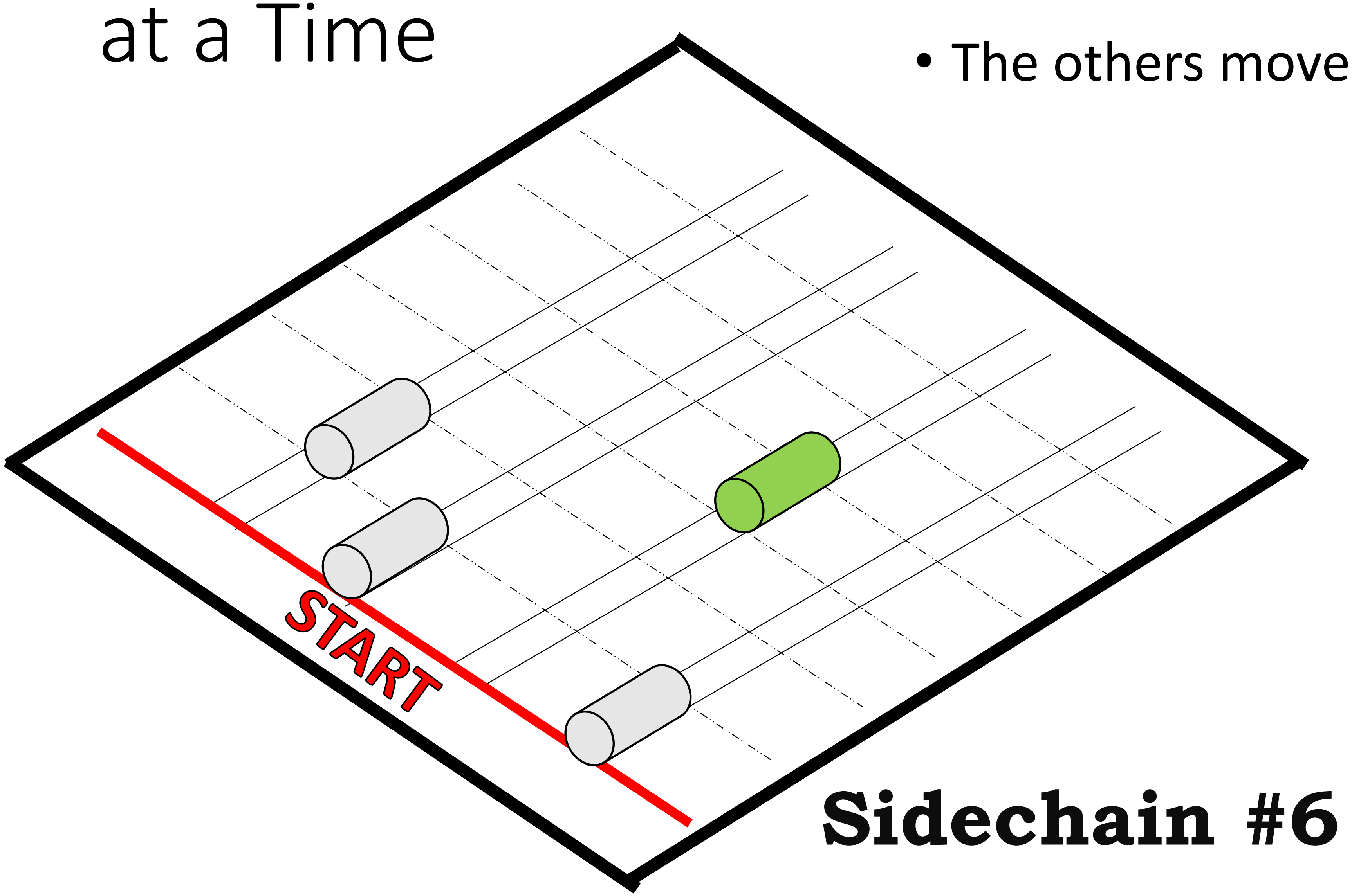
- The others move back.
- DoS prevention.



t = 10

Per Sidechain, Only One Traincar can advance at a Time

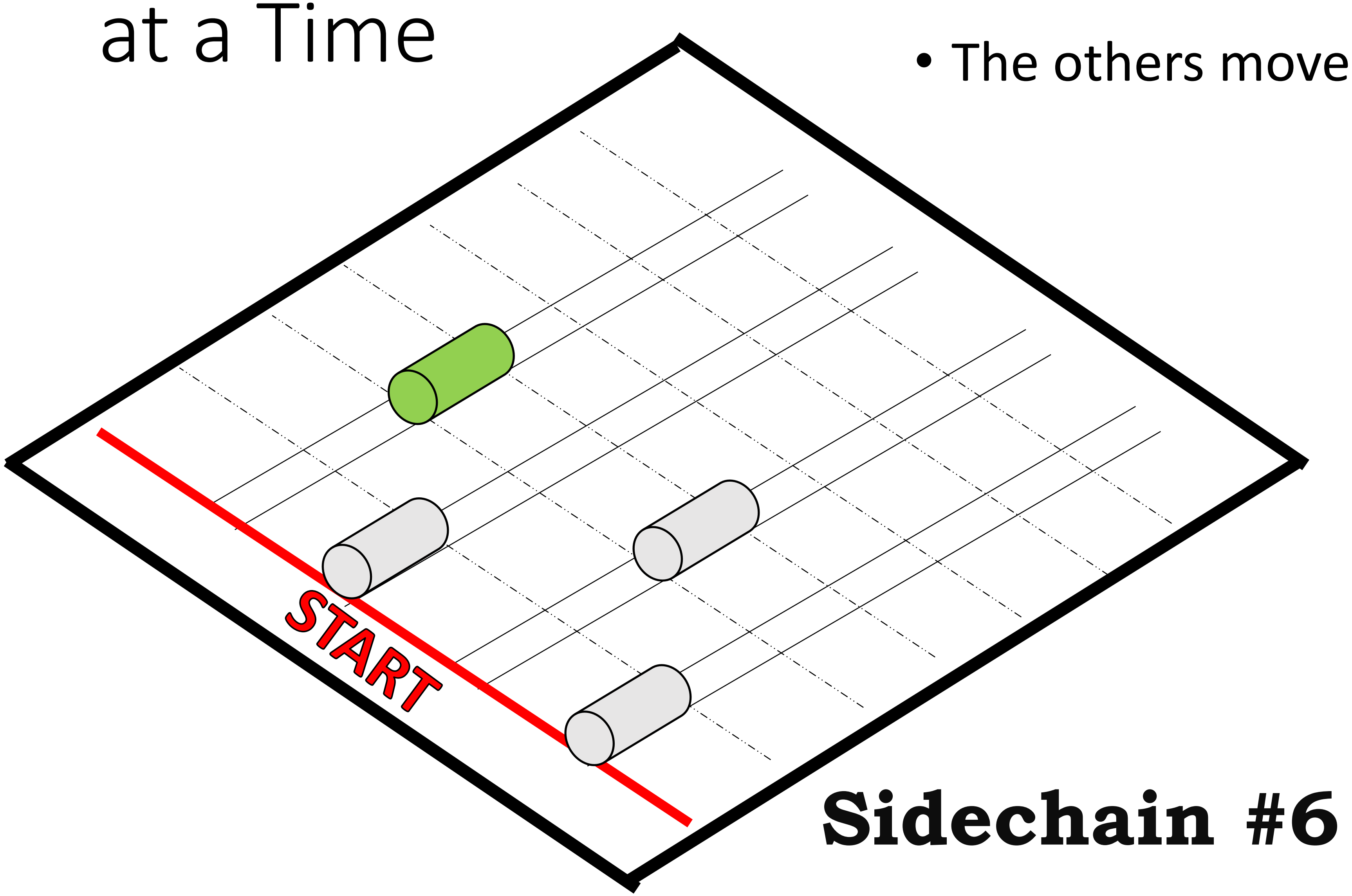
- The others move back.



t = 11

Per Sidechain, Only One Traincar can advance at a Time

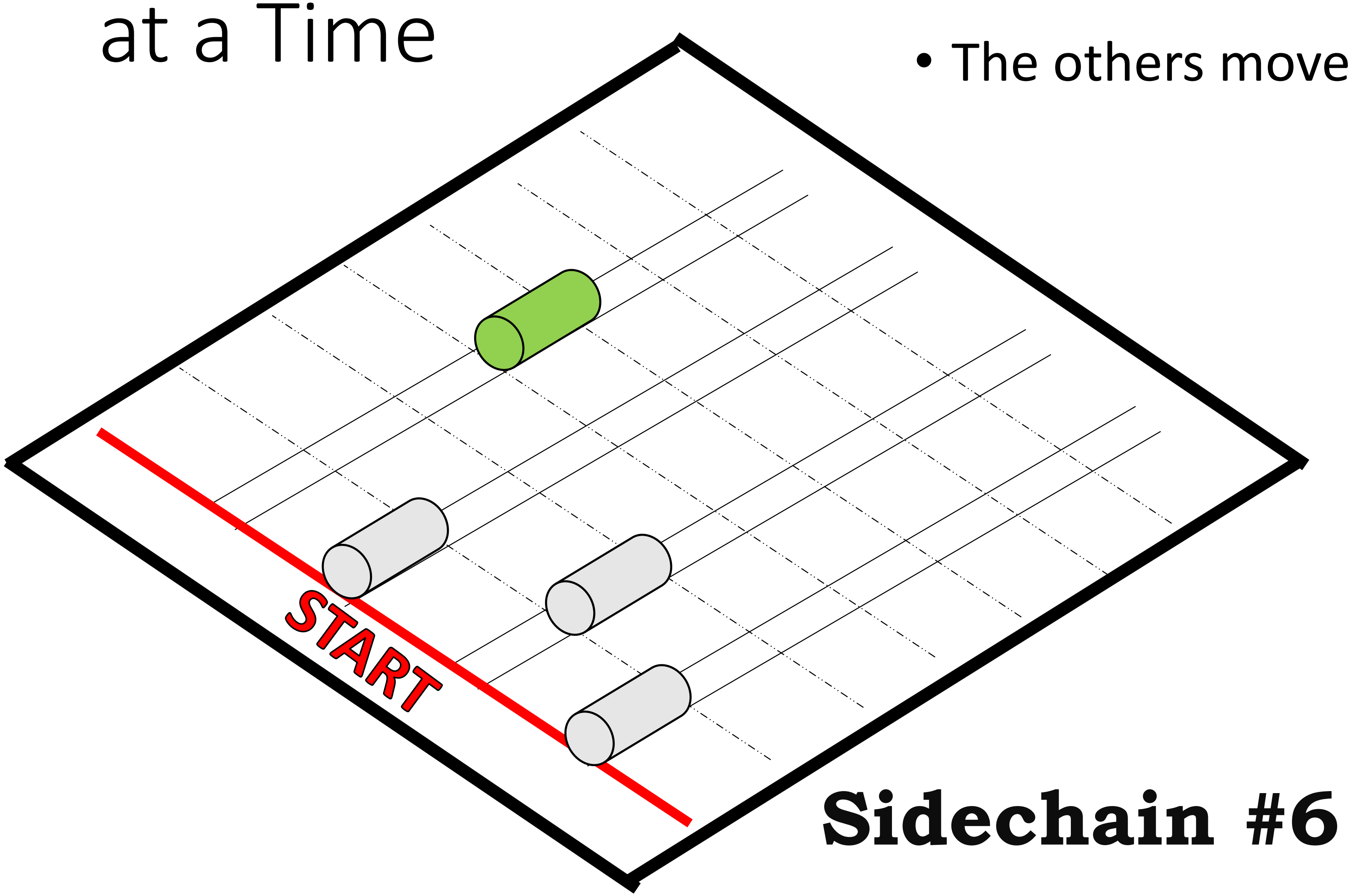
- The others move back.



t = 12

Per Sidechain, Only One Traincar can advance at a Time

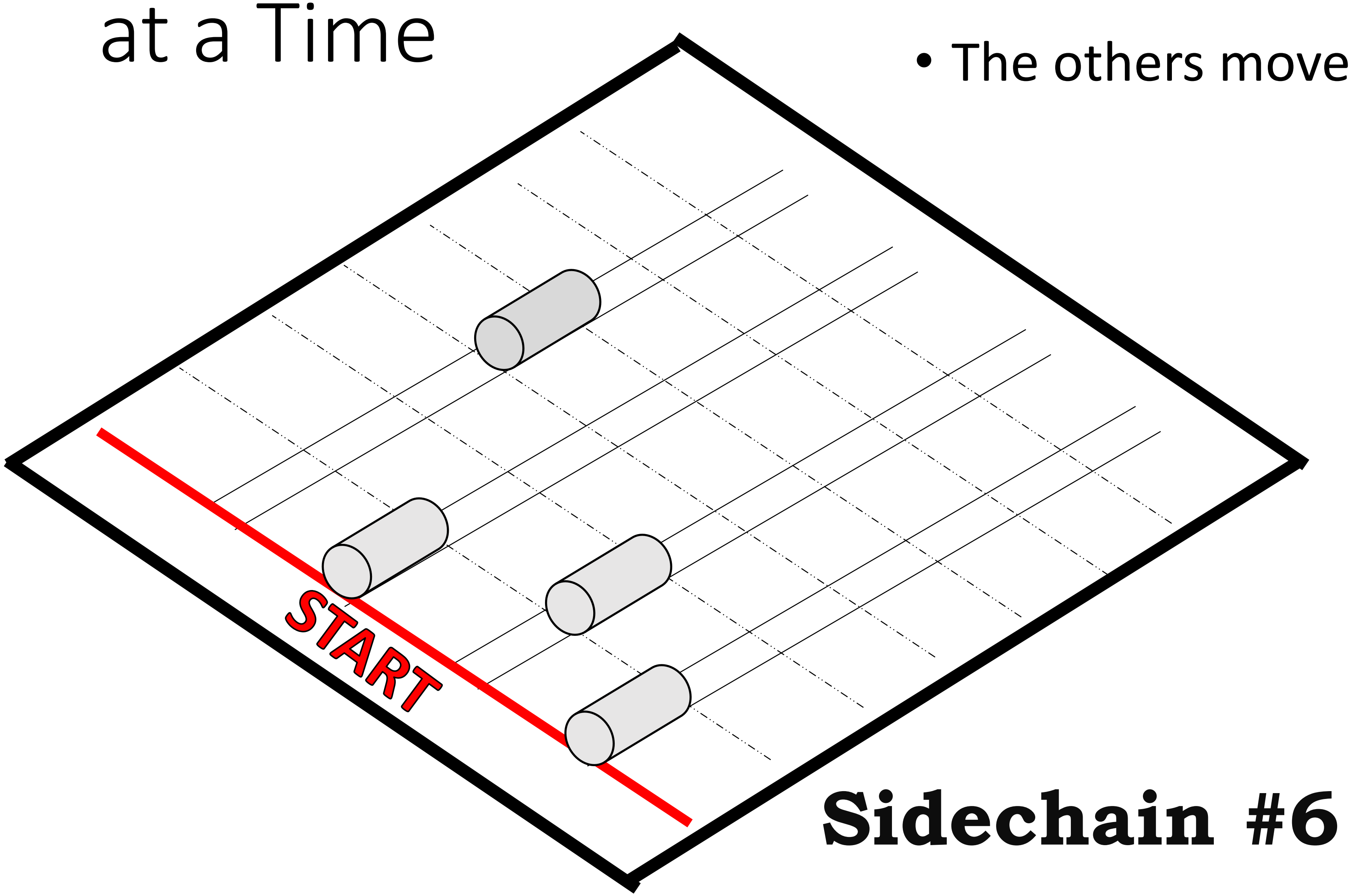
- The others move back.



t = 13

Per Sidechain, Only One Traincar can advance at a Time

- The others move back.



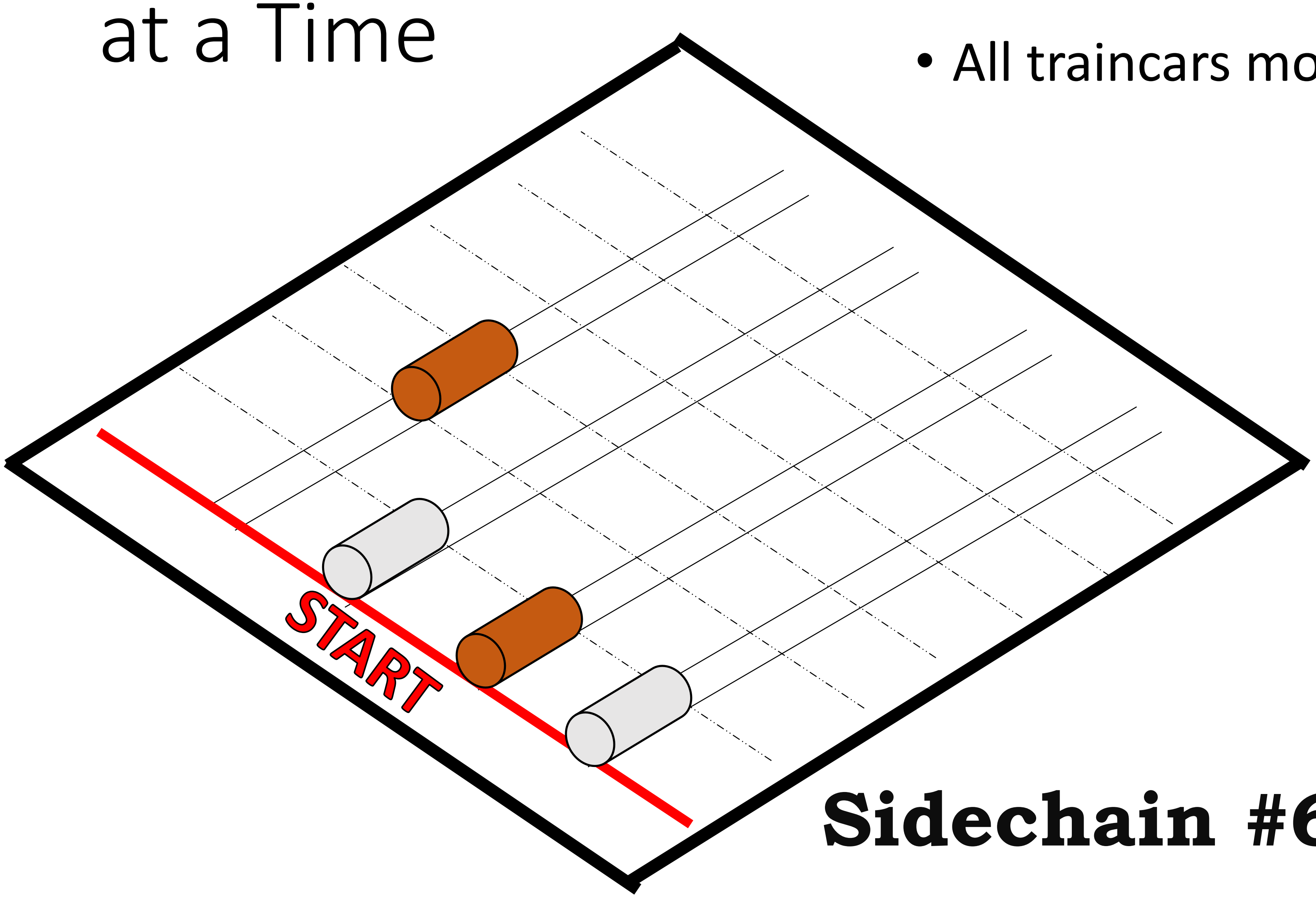
Abstain

t = 14

Sidechain #6

Per Sidechain, Only One Traincar can advance at a Time

- All traincars move back.

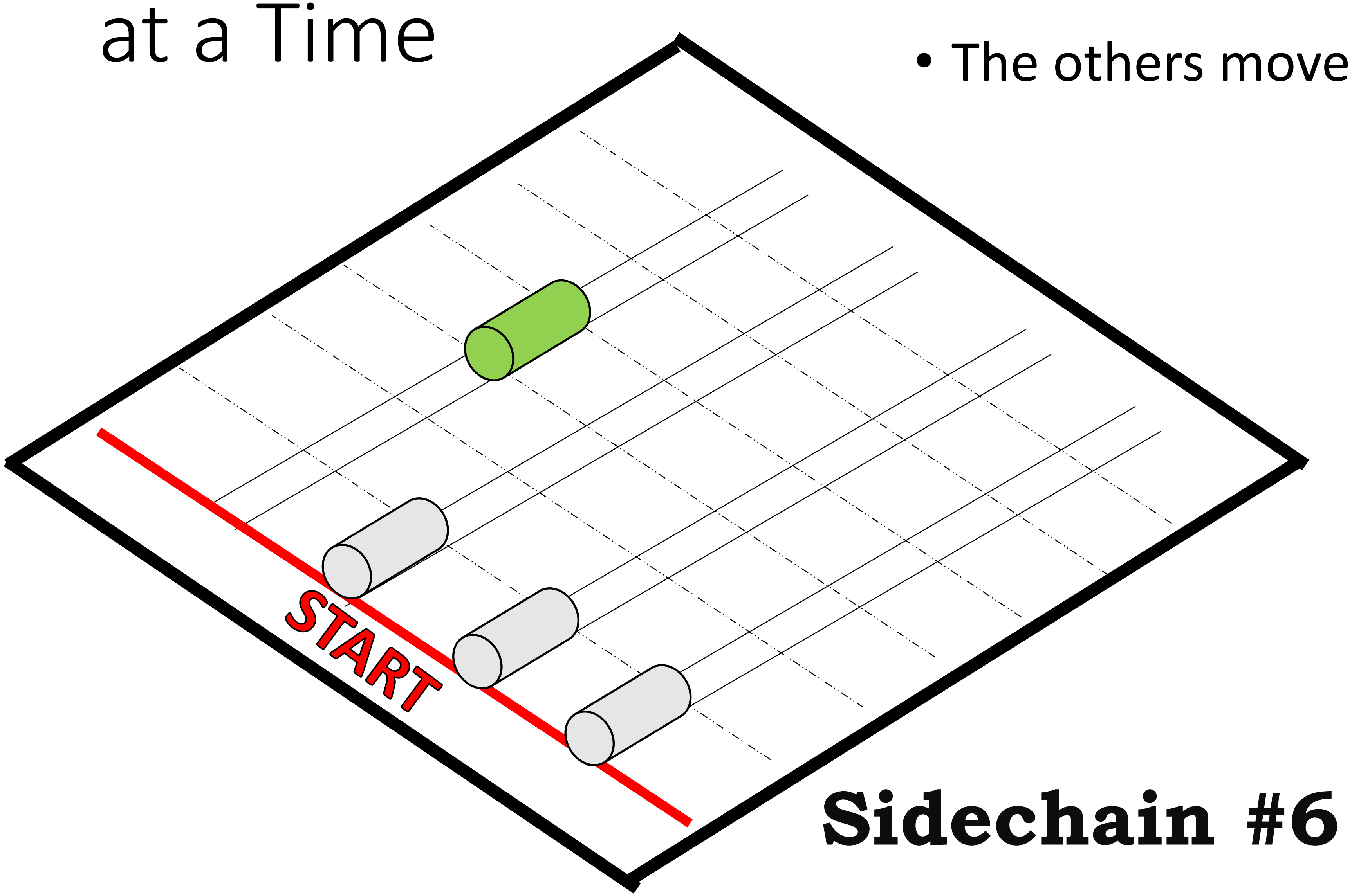


Alarm

t = 15

Per Sidechain, Only One Traincar can advance at a Time

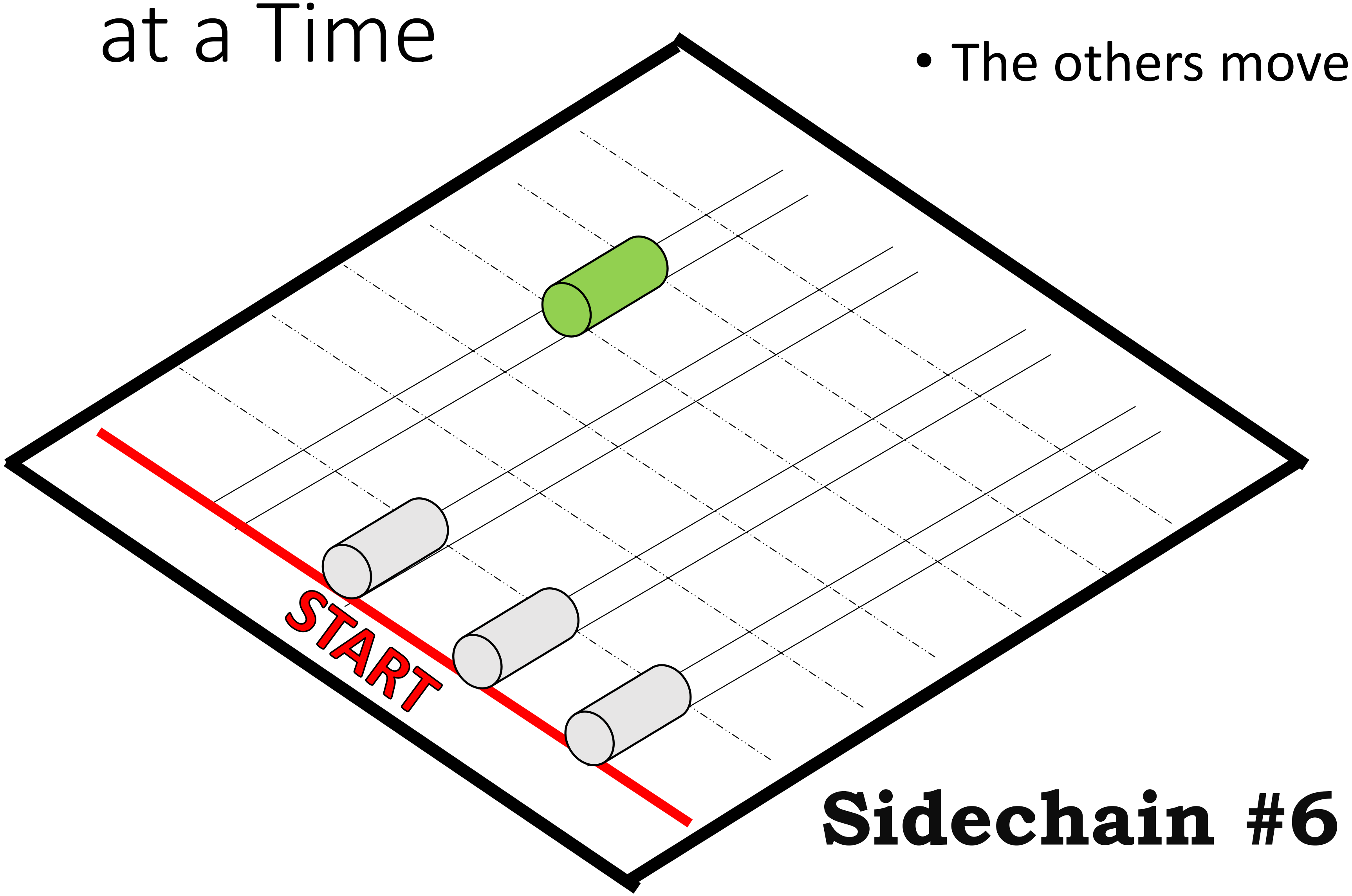
- The others move back.



t = 16

Per Sidechain, Only One Traincar can advance at a Time

- The others move back.



t = 17

Blind Merged Mining

- Will explain it in a second.

Two Big Critiques

1. “Miners can steal”
2. “Increased likelihood of mainchain txn-censorship.”

Critique #1

- **“Miners can steal”**
  - (Nothing guarantees that the 32 bytes that win the race, will be the 32 bytes that the sidechain full nodes sent.)
  - The act of moving a traincar forward, only “costs” the miner the opportunity to move any other traincar forward.
- *Increased likelihood of mainchain txn-censorship.*

“Miners Can Steal” – Response

1.
2.
3.
4.
5.

“Miners Can Steal” – Response

1. Would you prefer mandatory hard forks? (Or Altcoins?)
2.
3.
4.
5.

“Miners Can Steal” – Response

1. Would you prefer mandatory hard forks? (Or Altcoins?)
2. Theft is: transparent, 32-bytes, takes 3-6 months. MC enforced.
3.
4.
5.

“Miners Can Steal” – Response

1. Would you prefer mandatory hard forks? (Or Altcoins?)
2. Theft is: transparent, 32-bytes, takes 3-6 months. MC enforced.
3. Evict bad SCs. No loitering! No blockchain-crime!
4.
5.

“Miners Can Steal” – Response

1. Would you prefer mandatory hard forks? (Or Altcoins?)
2. Theft is: transparent, 32-bytes, takes 3-6 months. MC enforced.
3. Evict bad SCs. No loitering! No blockchain-crime!
4. Use of the word “can” = does not understand Bitcoin/blockchain.
5.

“Miners Can Steal” – Response

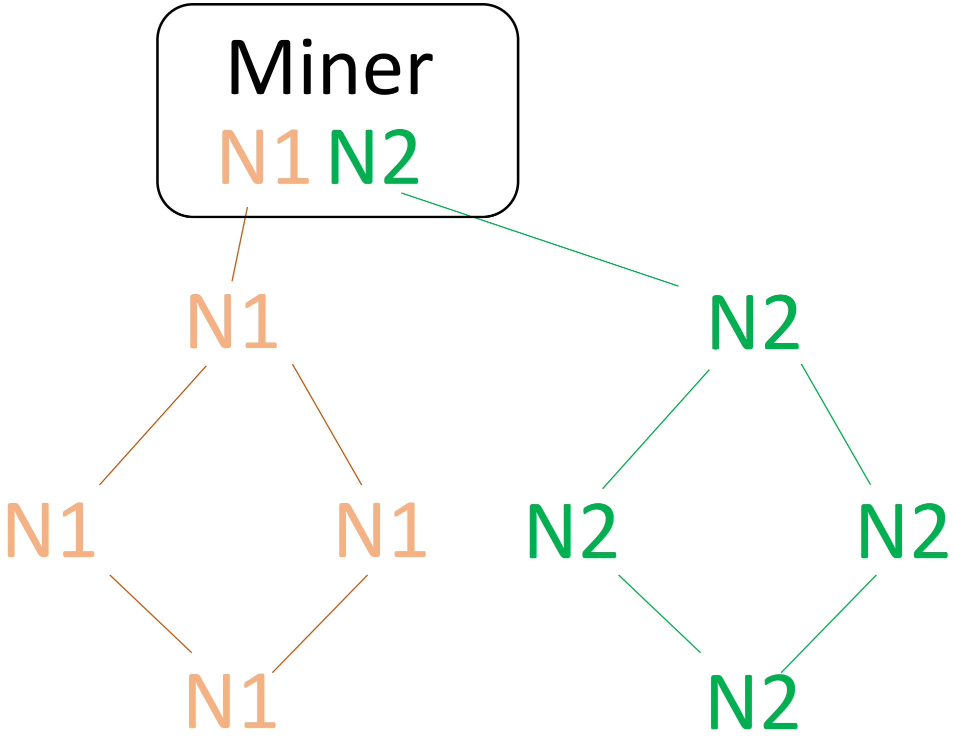
1. Would you prefer mandatory hard forks? (Or Altcoins?)
2. Theft is: transparent, 32-bytes, takes 3-6 months. MC enforced.
3. Evict bad SCs. No loitering! No blockchain-crime!
4. Use of the word “can” = does not understand Bitcoin/blockchain.
5. Let people make their own mistakes. It doesn’t affect you!

Critique #2

- *“Miners can steal”*
- **Increased likelihood of mainchain txn-censorship.**
  1. Sidechain(s) node costs = 5 (M $ per year)
  2. Sidechain revenues = 100 (M $ per year)
  3. Miner with 4% hashrate, must join larger pool.
  4. All pool operators must eventually run all SCs.
  5. Burdensome SC-software forces pools to run in large datacenters, making them easy targets for coercion.
  6. Regulators will be able to force pools to exclude some mainchain txns from the mainchain.

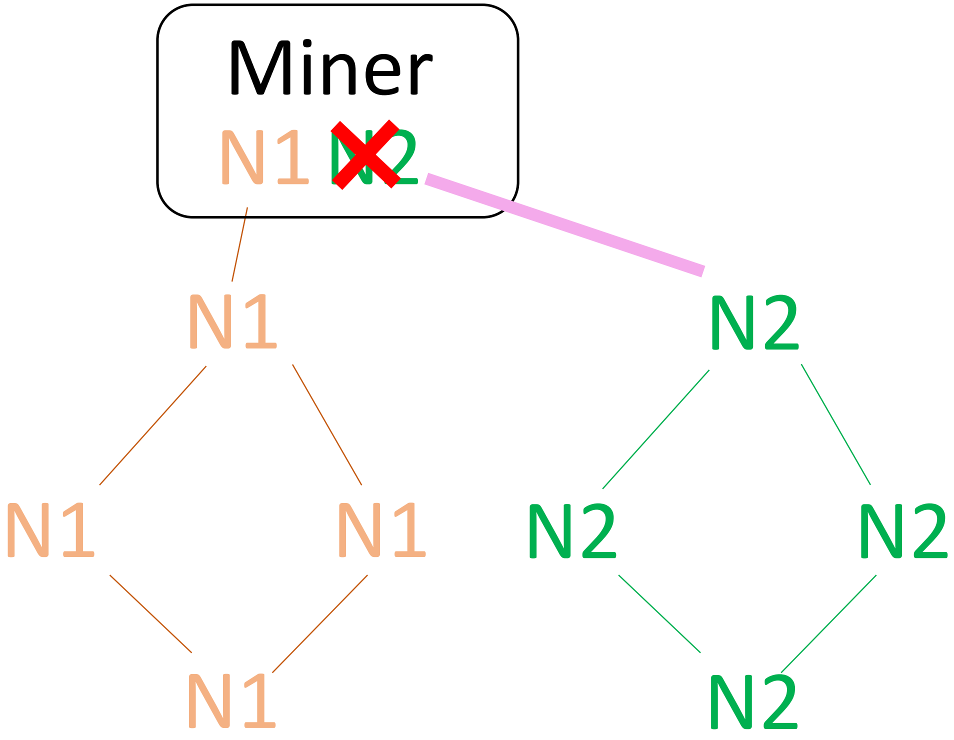
Regular Merged Mining

Miners must run a full node for each chain.



Blind Merged Mining

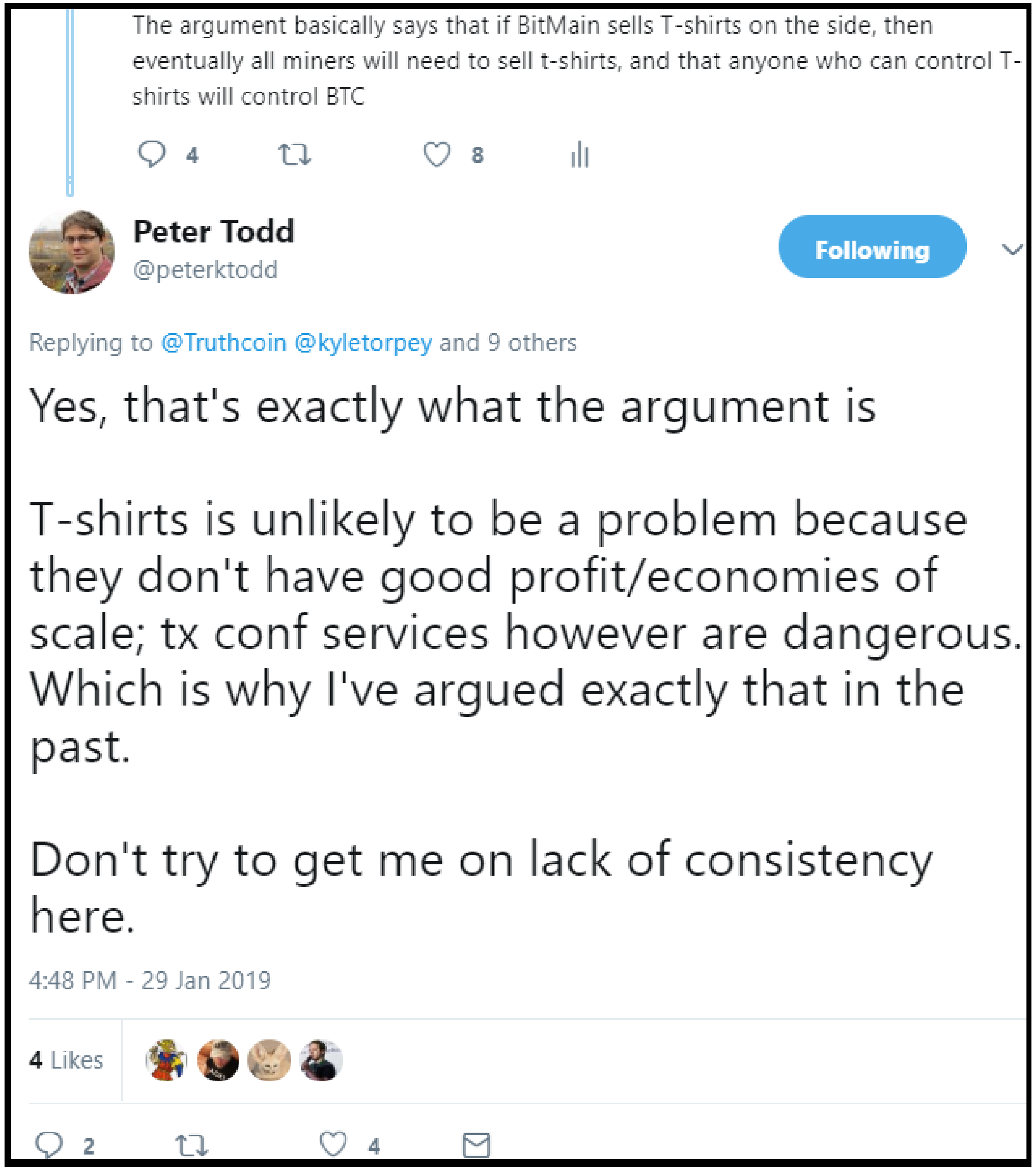
Miners do NOT run SC nodes, but still get 100% fee-profits.



- Much less data exchanged.
- 100% of network → small fixed amount of data

5 Reasons Why It’s Nonsense, Anyway

1.
2.
3.
4.
5.



The argument basically says that if BitMain sells T-shirts on the side, then eventually all miners will need to sell t-shirts, and that anyone who can control T-shirts will control BTC

Peter Todd
@peterktodd

Replying to @Truthcoin @kyletorpey and 9 others

Yes, that's exactly what the argument is

T-shirts is unlikely to be a problem because they don't have good profit/economies of scale; tx conf services however are dangerous. Which is why I've argued exactly that in the past.

Don't try to get me on lack of consistency here.

4:48 PM - 29 Jan 2019

5 Reasons Why It's Nonsense, Anyway

1. Inducement != Slavery; Argument Contradicts Itself
2.
3.
4.
5.

5 Reasons Why It’s Nonsense, Anyway

1. Inducement != Slavery; Argument Contradicts Itself
2. Caring about miner-comfort = does not understand Bitcoin.
3.
4.
5.

5 Reasons Why It’s Nonsense, Anyway

1. Inducement != Slavery; Argument Contradicts Itself
2. Caring about miner-comfort = does not understand Bitcoin.
3. Txn-censorship is a privacy issue. Not pools/SCs.
4.
5.

5 Reasons Why It’s Nonsense, Anyway

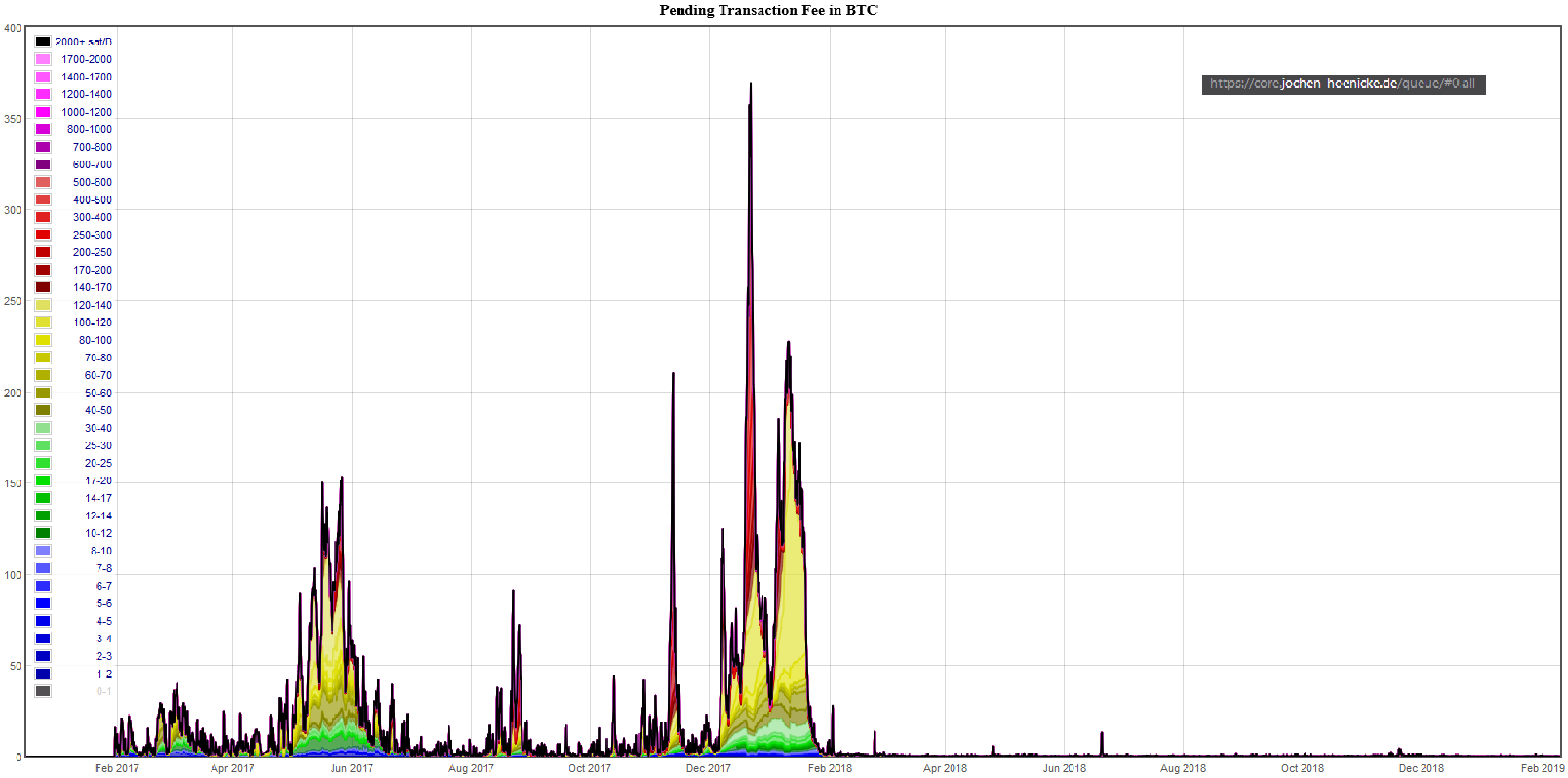
1. Inducement != Slavery; Argument Contradicts Itself
2. Caring about miner-comfort = does not understand Bitcoin.
3. Txn-censorship is a privacy issue. Not pools/SCs.
4. We need those MM fees!!
5.

Security Budget over next 40 yrs, if Fees are Zero

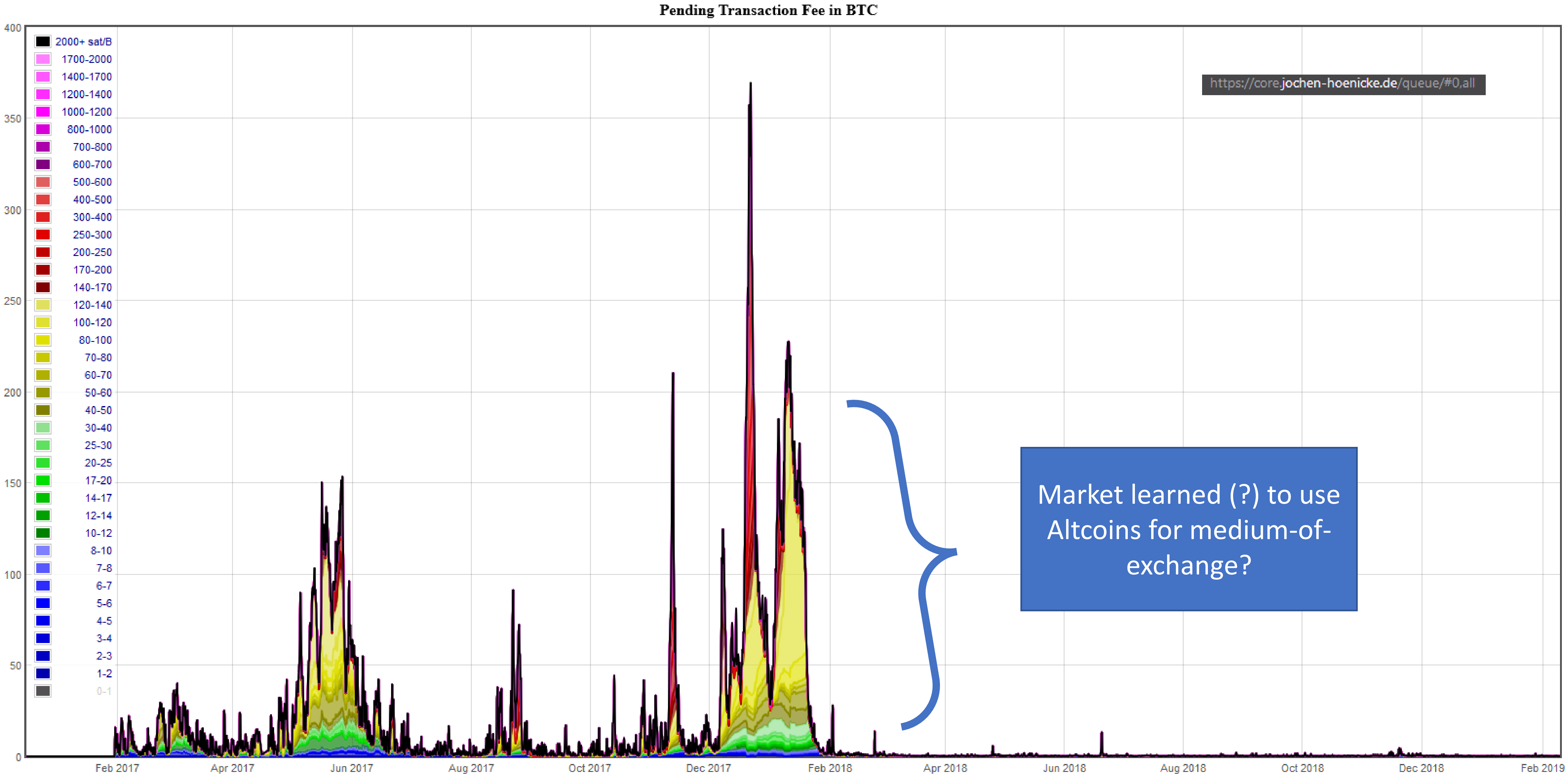
Year	Subsidy	Exchange Rate (theoretical maximum)	Exchange Rate (market-imputed)	BTC Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio	
	from protocol	x_2017 = $11.22M, growth = 1.077	x_2016 = $700, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.i.) * 6 * 24 * 365 * (1/1e9)	x_2015 = 637, growth = 1.047	Security B. / Defense B.	
2008	50	$2,725,960	$0	$0.00	$461.76	0.000	"Indifference" Epoch
2012	25	$3,671,828	$100	$0.13	$554.95	0.000	
2016	12.5	$4,945,897	$700	$0.46	$666.96	0.001	
2020	6.25	$6,662,050	$4,900	$1.61	$801.57	0.002	
2024	3.125	$8,973,683	$75,000	$12.32	$963.36	0.013	
2028	1.5625	$12,087,419	$800,000	$65.70	$1,157.79	0.057	"Healthy" Epoch
2032	0.78125	$16,281,574	$15,000,000	$615.94	$1,391.47	0.443	
2036	3.9E-01	$21,931,039	$21,931,039	$450.27	$1,672.32	0.269	
2040	2.0E-01	$29,540,785	$29,540,785	$303.25	$2,009.85	0.151	"Decline" Epoch
2044	9.8E-02	$39,790,999	$39,790,999	$204.24	$2,415.50	0.085	
2048	4.9E-02	$53,597,887	$53,597,887	$137.55	$2,903.02	0.047	
2052	2.4E-02	$72,195,560	$72,195,560	$92.64	$3,488.94	0.027	
2056	1.2E-02	$97,246,350	$97,246,350	$62.39	$4,193.13	0.015	

Completely Different Realms

Revenue-Source	Block Subsidy (12.5 BTC)	Transaction Fees
Meme	Store of Value	Medium of Exchange
Slogan	“Digital Gold”	“P2P Cash for the World”
Supply and Demand	…of BTC	…of block space
Critical Price	$ (PPP) / Bitcoin	$ (PPP) per byte
If BTC price = moon…	…Security Goes Up	*…Unaffected*



https://core.jochen-hoenicke.de/queue/#0,all



Market learned (?) to use Altcoins for medium-of-exchange?

Completely Different Realms

Revenue-Source	Block Subsidy (12.5 BTC)	Transaction Fees
Meme	Store of Value	Medium of Exchange
Slogan	“Digital Gold”	“P2P Cash for the World”
Supply and Demand	…of BTC	…of block space
Critical Price	$ (PPP) / Bitcoin	$ (PPP) per byte
If BTC price = moon…	…Security Goes Up	*…Unaffected*

Bottom Line: Today, fees = $200/block ; a mere $ 10,512,000 per year.

Without MM, they might plausibly NEVER be higher than that.

10M = $ 0.01 billion
= joke

Security Budget over next 40 yrs, if Fees are Zero

Year	Subsidy	Exchange Rate (theoretical maximum)	Exchange Rate (market-imputed)	BTC Security Budget (billions per year)	USA Defense Spending (billions per year)	Safety Ratio	
	from protocol	x_2017 = $11.22M, growth = 1.077	x_2016 = $700, growth = 1.6265; blended with maximum	= Subsidy * Exchange Rate (m.i.) * 6 * 24 * 365 * (1/1e9)	x_2015 = 637, growth = 1.047	Security B. / Defense B.	
2008	50	$2,725,960	$0	$0.00	$461.76	0.000	"Indifference" Epoch
2012	25	$3,671,828	$100	$0.13	$554.95	0.000	
2016	12.5	$4,945,897	$700	$0.46	$666.96	0.001	
2020	6.25	$6,662,050	$4,900	$1.61	$801.57	0.002	
2024	3.125	$8,973,683	$75,000	$12.32	$963.36	0.013	
2028	1.5625	$12,087,419	$800,000	$65.70	$1,157.79	0.057	"Healthy" Epoch
2032	0.78125	$16,281,574	$15,000,000	$615.94	$1,391.47	0.443	
2036	3.9E-01	$21,931,039	$21,931,039	$450.27	$1,672.32	0.269	
2040	2.0E-01	$29,540,785	$29,540,785	$303.25	$2,009.85	0.151	"Decline" Epoch
2044	9.8E-02	$39,790,999	$39,790,999	$204.24	$2,415.50	0.085	
2048	4.9E-02	$53,597,887	$53,597,887	$137.55	$2,903.02	0.047	
2052	2.4E-02	$72,195,560	$72,195,560	$92.64	$3,488.94	0.027	
2056	1.2E-02	$97,246,350	$97,246,350	$62.39	$4,193.13	0.015	

5 Reasons Why It’s Nonsense, Anyway

1. Inducement != Slavery; Argument Contradicts Itself
2. Caring about miner-comfort = does not understand Bitcoin.
3. Txn-censorship is a privacy issue. Not pools/SCs.
4. We need those MM fees!!
5.

5 Reasons Why It’s Nonsense, Anyway

1. Inducement != Slavery; Argument Contradicts Itself
2. Caring about miner-comfort = does not understand Bitcoin.
3. Txn-censorship is a privacy issue. Not pools/SCs.
4. We need those MM fees!!
5. Vanilla MM cannot be stopped. So, get used to it.

Conclusion

- Goals
  - Defeat Altcoins
  - Resolve Scalability Conflict, permanently.
  - More innovation.
- Call to Action
  - Join telegram group: **t.me/DcInsiders**
  - Help us test.
  - Stop FUD – I will post refutations to Critique 1 and 2, on website
  - **Drivechain.info**

Agen a

1. Sidechai niversal Altcoin Simulation (and Cor ssion)
2. How it
3. Critiques o Sidechains
4. Sidechain Privatization (“Interchain combat” and “flipped work”).
   - Name-leeching.
   - Oracle reputation-leeching.
   - Fee-leeching.

Agenda

1. Sidechains: Universal Altcoin Simulation (and Compression)
2. How it works
3. Critiques of Sidechains
4. Sidechain Privatization (“Interchain combat” and “flipped work”).
   - Name-**leeching**.
   - Oracle reputation-**leeching**.
   - Fee-**leeching**.

Leeching

Of all types of ***blockchain interference***, generally the easiest to understand.

“Miners Can Steal” – Response

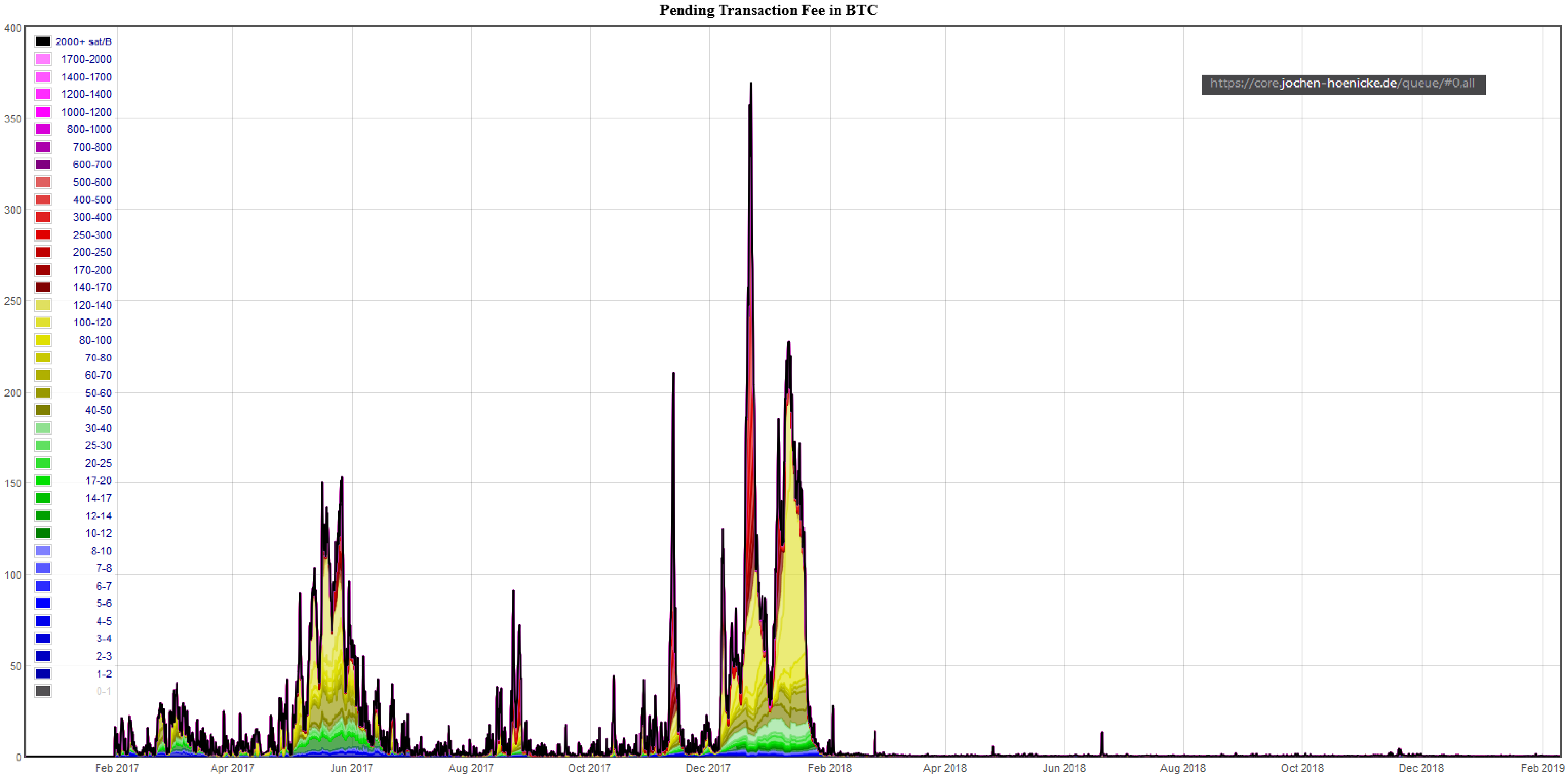
1. Would you prefer mandatory hard forks? (Or Altcoins?)
2. Theft is: transparent, 32-bytes, takes 3-6 months. MC enforced.
3. Evict bad SCs. No loitering! No blockchain-crime!
4. Use of the word “can” = does not understand Bitcoin/blockchain.
5. Let people make their own mistakes. It doesn’t affect you!

If miners couldn’t get rid of bad SCs, could not kill leeches. They would prevent really cool contracts from existing.

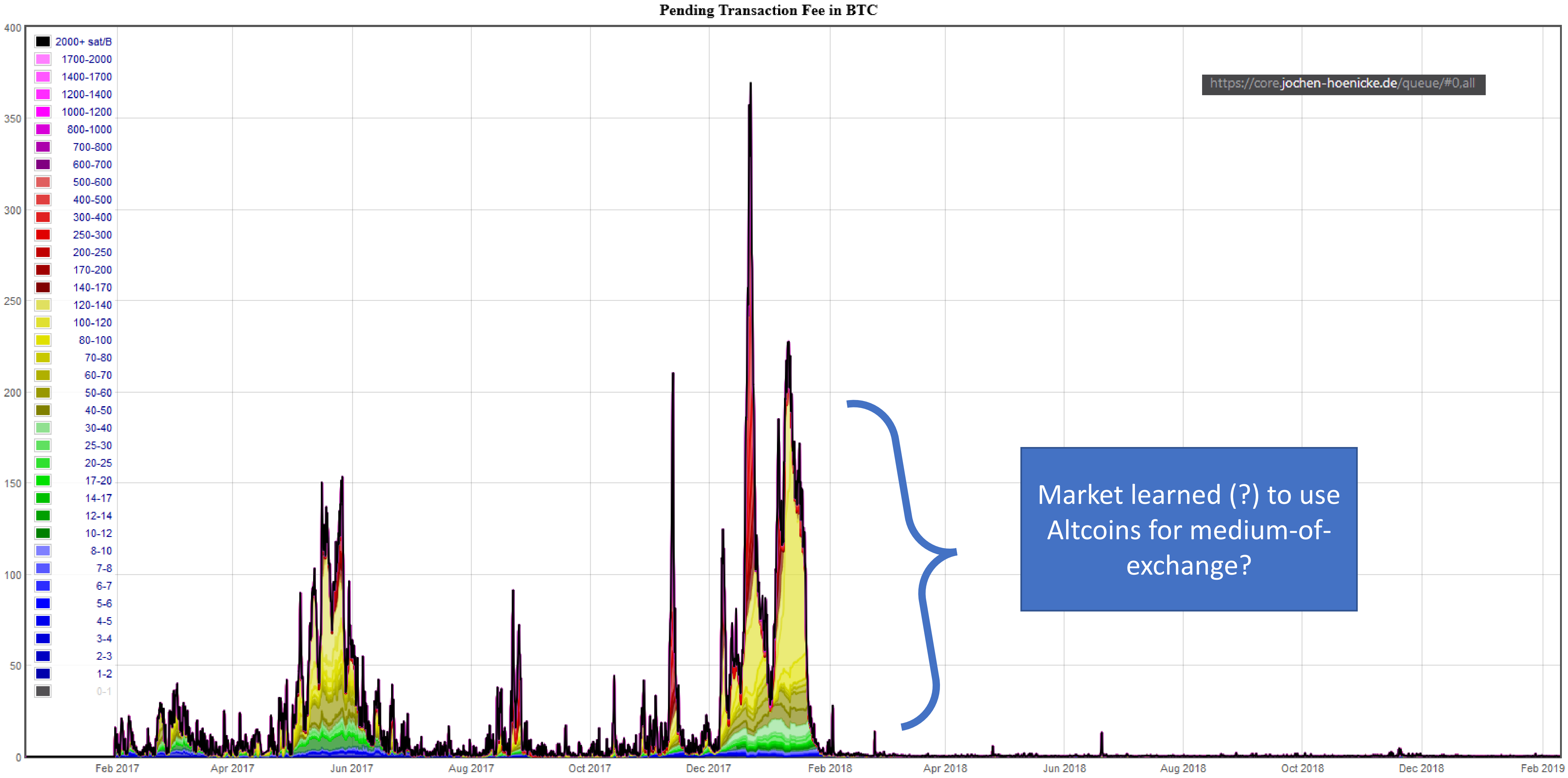
(Fortunately, “miners can” get rid of them.)

Name Leeching

- Someone makes an identity sidechain. You register a name, for example “Bitcoin.com”.
- Someone makes a *second* identity sidechain, and registers “Bitcoin.com” over there.



https://core.jochen-hoenicke.de/queue/#0,all

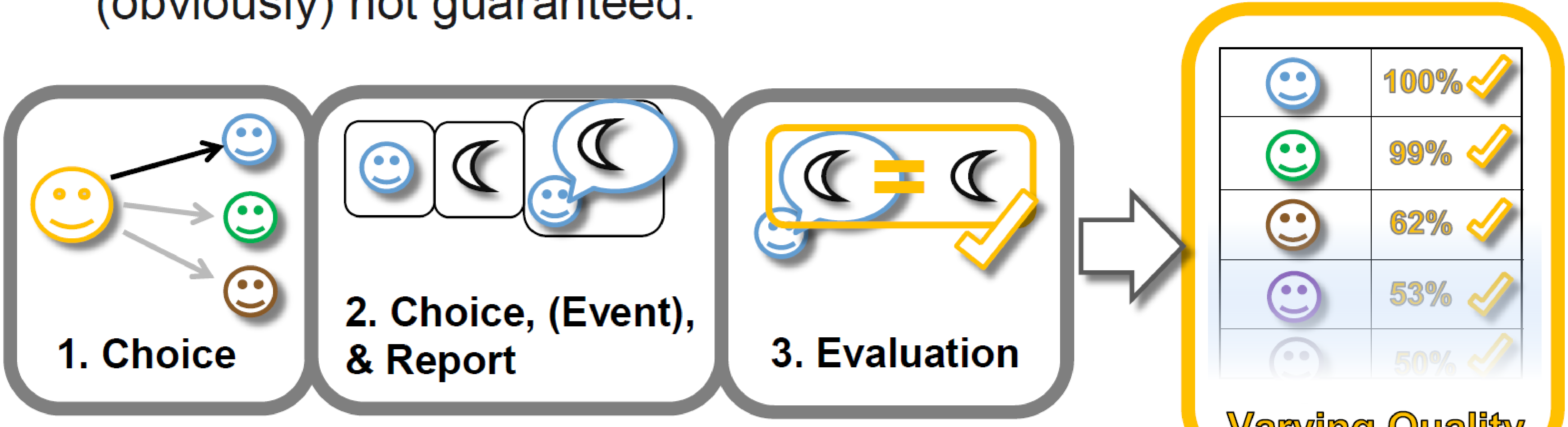


Market learned (?) to use Altcoins for medium-of-exchange?

Corporation Model Breaks Sometimes

Ultimately, oracles ***need*** to vary in quality (because we must choose them pre-report, and evaluate them post-report).

We necessarily ‘trust’ them, mid-event. Performance is (obviously) not guaranteed.



1. Choice

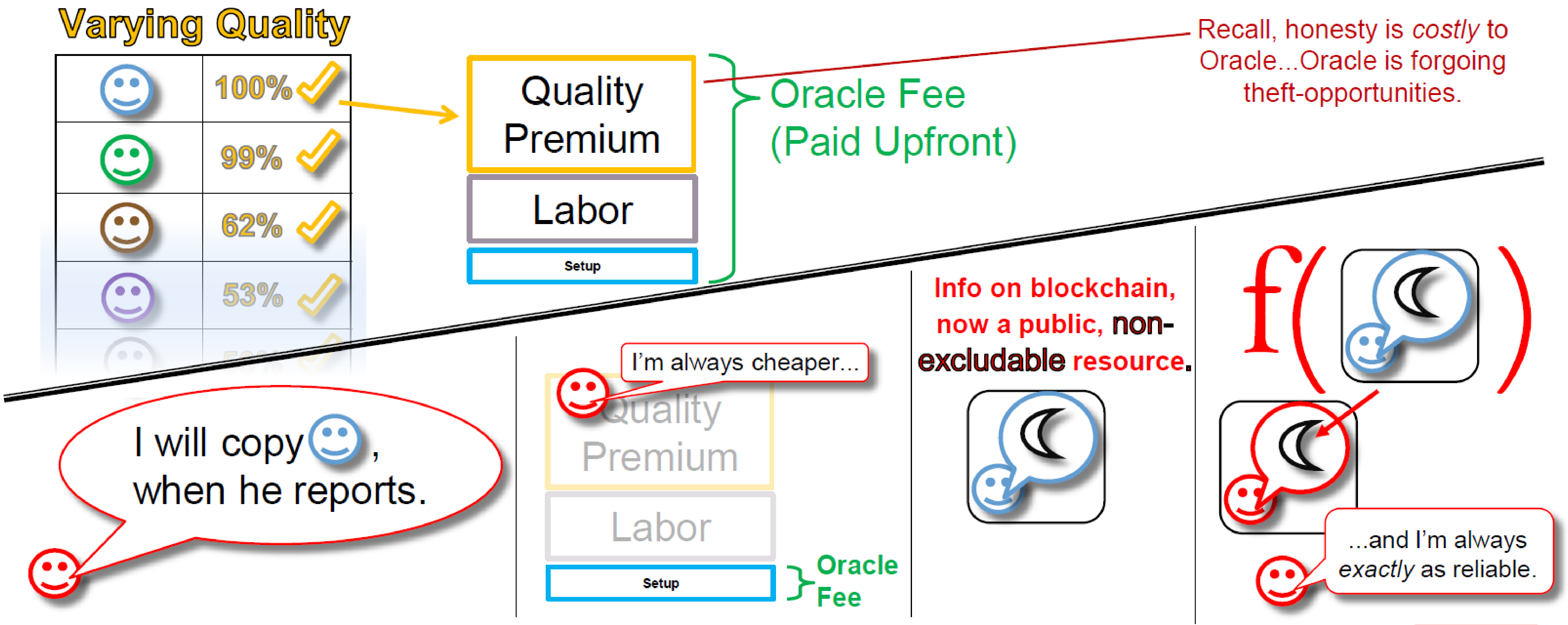
2. Choice, (Event), & Report

3. Evaluation

Varying Quality

Multiple oracles

To Purchase Quality, Need pseduo-“©”



Varying Quality

☺	100% ✓
☺	99% ✓
☺	62% ✓
☺	53% ✓
☺	50% ✓

Quality Premium

Labor

Setup

Oracle Fee (Paid Upfront)

Recall, honesty is *costly* to Oracle...Oracle is forgoing theft-opportunities.

I will copy ☺, when he reports.

I’m always cheaper...

Quality Premium

Labor

Setup

Oracle Fee

Info on blockchain, now a public, non-excludable resource.

f( )

...and I’m always *exactly* as reliable.

- Result: “crypto-reputation” is impossible (all always 50% ✓) . No different from trusting website.
- **Other *impossible* things: all DACs, identity, fidelity bonds, financial markets.**
- In contrast, a single ‘mega-contract’ can (with entrants excluded) “coordinate” payment-events and oracle-quality events. It can *force* a mapping from quality to $.

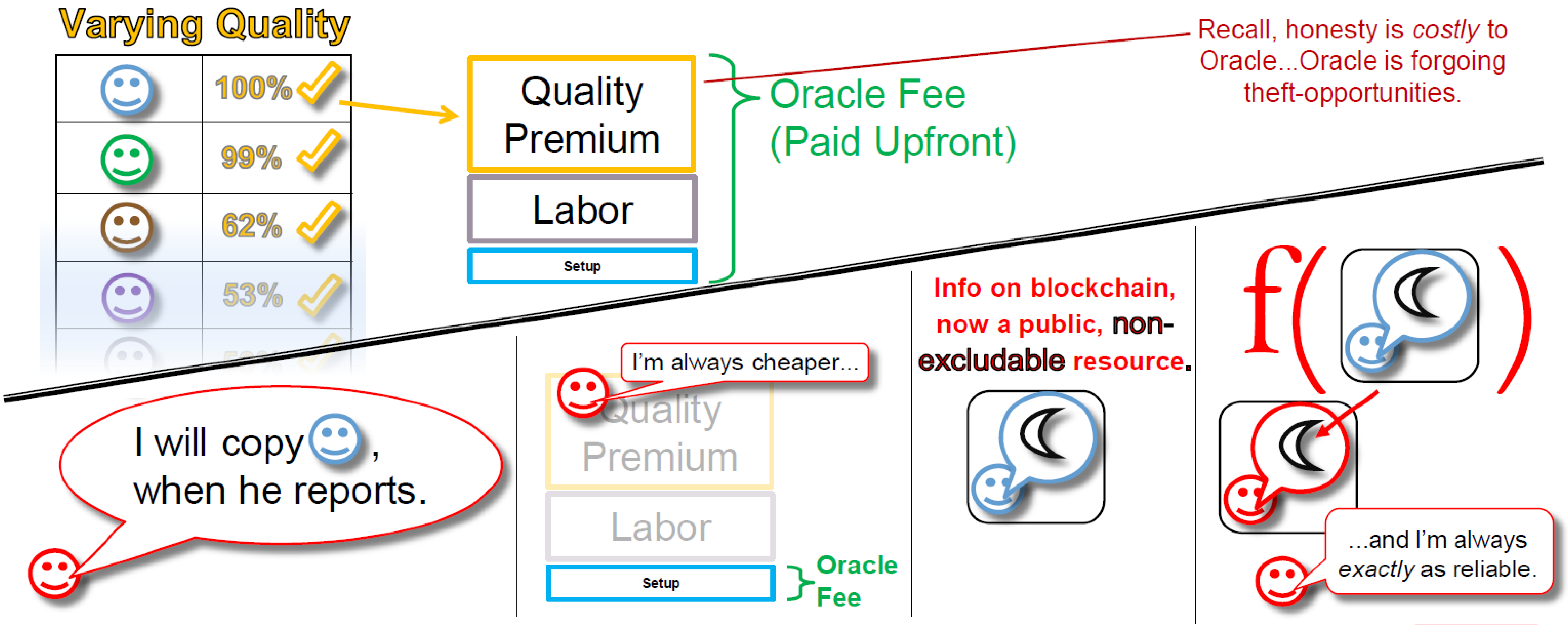
Quality varies, payments don’t co-vary!

Can’t buy quality!

☹

OUT OF BUSINESS

To Purchase Quality, Need pseduo-"©"



Varying Quality

☺	100% ✓
☺	99% ✓
☺	62% ✓
☺	53% ✓
☺	50% ✓

Quality Premium

Labor

Setup

Oracle Fee (Paid Upfront)

Recall, honesty is *costly* to Oracle...Oracle is forgoing theft-opportunities.

I will copy ☺, when he reports.

I'm always cheaper...

Quality Premium

Labor

Setup

Oracle Fee

Info on blockchain, now a public, non-excludable resource.

f( )

...and I'm always *exactly* as reliable.

- Result: "crypto-reputation" is impossible (all always 50% ✓) . No different from trusting website.
- **Other *impossible* things: all DACs, identity, fidelity bonds, financial markets.**
- In contrast, a single 'mega-contract' can (with entrants excluded) "coordinate" payment-events and oracle-quality events. It can *force* a mapping from quality to $.

Quality varies, payments don't co-vary!

Can't buy quality!

☹ OUT OF BUSINESS

Questions