Banter

Last...but not least...

I'd like to thank the opening bands ...whoever they were. : )

Slide 1

Hi everyone, I'm Paul Sztorc.

Thanks for having me.

Slide 2

I am going to try to

talk about something new,

(in the second half)

but first I want to

talk about two

old

sidechain beliefs.

Slide 3

The first

is that "sidechains

...affect mainchain miners".

I will explain it in a moment.

But it is significant,

because,

if \*true\*,

this theory implies

that we need to tightly control

the software

that users and miners

decide to run.

It is also important,

because it is a kind of

last trench

of the Sidechain Opponent.

Sidechain-opponents

do admit

that SC-nodes leave MC-nodes alone.

(So the node side is not in dispute.)

Snapchat

Only this mining edge is in dispute.

Slide 4

The objection is that:

1. SCs offer a conditional payment to miners

2. the miners have no choice to accept,

(so the conditions are mandatory)

3. The conditions are bad.

Therefore, sidechains are bad for Bitcoin.

The logic is that

as miner profit-margins

narrow over time,

miners will become

more and more desperate.

If some

miners

are earning fees

from a SC node,

and other miners are not,

then equilibrium difficulty

will increase,

...and miners either

will mine the SC

or else they will

go out of business.

And then second,

you just imagine:

that something is bad

about the node software

they're running.

So very popular SC

high fees

But something bad about running it

And its mandatory.

Slide 5

A second belief, is that:

"SCs allow miners to steal BTC".

This perspective holds

that user's coins are

currently

protected by powerful cryptography.

--backed by math-- you know.

And SCs

frivolously

take it out of this

realm,

and put it into a "flaky"

game-theoretic realm.

Woah what's that?

its practically the humanities.

It's like saying that Bitcoin

should be secured by "love"

or "friendship" or something.

Take it out of the engineering dept

and put it in the sociology dept.

Anyway,

those are the two beliefs:

SCs affect miners,

and SCs are irresponsible

because they open

the user's BTC up to theft.

Slide 6

Now,

what I'd like to say first,

is that these two points

are -kind of- opposites of each other.

They are similar,

in a bad way:

the first, suggests

that we need to tightly control

the software that users and miners run,

because it might,

be bad software.

( they might run bad software

that would affect the miners)

the second, suggests

that we need to tightly control,

the types of txns that users make,

because they might send their BTC

to an unwise destination.

Despite being similar in that bad sense,

I think that they have

a kind of opposite-ness to them.

The first claims

that SC do something to miners;

and the second one claims

that miners can do something to SCs.

The first has

miners as being weak, docile,

and hopelessly manipulated

against their will

by the Users of the SC.

The second says

that users are in the position of despair,

and miners are all-powerful force,

just moments away from crushing the SC

and making off with all of the BTC

that was foolishly

deposited there.

So that's kind of funny.

Of course,

...

the fact ...

that they are

kind of at odds with each other,

does nothing to prevent them

from

both being

\*completely\* false.

Slide 7

image: anything can affect miner incentives;

51% hashrate can steal from anything

The refutation

of the first

is to notice

that anything

could have done that thing to miners;

and (similarly)

the refutation

of the second

is to notice

that miners can

already do that thing

to everything else.

In both cases

the word "sidechain"

could be more-accurately

substituted with anything,

or even nothing.

Let us return to the first belief.

Slide 8

restore image of three-part argument

overlay:

image: P ; N ; lines connecting multiple H's to Ps | N [BTC] line P, line Hs ;; Ns with dashed line to P

Belief 1: "SCs affect miner incentives"

Now, already

the story of onerous nodes

contains a few falsehoods.

First and most obvious,

is that what we call "miners"

is actually two quite different groups,

the "hashers" and the "pool administrators".

Only the

pool administrators

run nodes.

The barriers to entry

(which is to say,

how quickly and easily

will they be replaced

if they screw up)

is low for both.

And only the pool administrator

would need to run

a new sidechain node --

the hashers need only

adopt

the same policy as always

which is to go with

whichever pool pays the most,

without really caring

how or why

the pool admin was paying so well.

In fact,

even the pool administrator

need not actually run

the SC node,

the admin could

merely have some relationship or arrangement

with any pre-existing nodes.

And a development of mine,

blind merged mining

would make such a relationship trustless.

Third,

adding sidechains is a soft fork,

so if premise #2 were true,

(ie, that miners have no choice but to accept),

then miners would also

have no choice

but to 'soft fork in' sidechains technology

whenever possible.

Users can try to stop them,

with some kind of UASF,

but miners can just try

over and over again

every block.

And the UASF

can only be done

a few times per year,

in my opinion.

(The UASF is not

socially scalable.)

But those quibbles

are not even close

to the optimal refutation

of this argument.

Since premise #1

is undeniably true,

and #3 is always possible by definition,

let us examine premise #2.

...and notice that this conditional payment

could be replaced

by \*any other conditional payment\*.

Slide 9

So: Chinese govt could announce "We will pay [$5 a month] to any miner [who reveals their mailing address]."

Anything lower than the SC txn fees + ER effect (ie, the "Sidechain Inducement") ; and anything arbitrarily worse than running a SC node.

or ... [US Federal Reserve] .. [$1 a year] .. [choose to obtain "mining licenses" from the FED (which come with arbitrary strings attached]

So,

in order to complain about SCs specifically,

you'd need to argue that

the SC's transaction fees

are somehow much more persuasive, per dollar,

than other arbitrary payments.

(They're somehow more enticing.)

But even if that were true,

and there was a

"premium for trustlessness",

then the FED could respond

by upping the magnitude of their incentive,

by doubling it to 2$ a year. Or 3$ a year.

( they can afford it. )

In point of fact,

I don't think it is true

-- all of the payments could be made in BTC,

so that's the same.

And while someone \*could\*

argue that,

at the time that the block is mined

SC txn fees are trustless,

that only matters in a world

where people don't trust

the government / FED to keep

its word.

But that is ridiculous because governments

have a very public brand...

...if the FED announces a policy

and commits to it,

and they follows through every single block,

for days on end,

then I think

the need for trust (in that scenario)

falls basically to zero.

So, the truth

is that miners will

reject conditional payments

if the conditions are excessively bad.

And this includes desperate, impoverished miners.

They will only accept if the conditions are good.

Therefore,

SC do not "affect" mainchain users.

Because,

even if a SC is merged mined,

it cannot make the miner's position

any more precarious

than it already is.

In fact it

can only increase

the equilbrium hashrate.

Sidechains are 100% opt-in,

and sidechain-use doesn't affect mainchain BTC transactions in any negative way.

Therefore,

there is no basis for opposing sidechains,

other than tyranny.

Supporting sidechains is \*free\*, for Bitcoin Core -- it is no different from supporting SegWit or CheckLockTimeVerify.

and it doesn't matter

if users try out a sidechain,

and it explodes or something,

or if funds are lost,

or stole by miners.

That is considered

acceptable \*and desirable\*.

As Nassim Taleb says,

you can't have an antifragile layer,

unless the layer beneath it

is explicitly fragile.

Furthermore,

if miners are allowed to steal SC funds,

then they are also allowed to threaten to steal SC funds.

Those are actually the same thing.

...which brings me back

to the second misconception...

Slide 10

... that "SC allow 51% miners to steal funds".

Which is also false,

key phrase being "SCs allow",

as I will now explain.

Miners can steal from a SC,

but that has nothing to do with SC-ness.

51% hashrate can steal from anything.

\* Image: "SCs \*allow\* 51% hashrate to steal coins" ;; "51% hashrate can steal coins (from Mainnet, Lightning, and SCs)".

Majority hashrate

controls the chain history,

and anyone

(including 51% hashrate)

can make new txns.

So,

miners have addition

and subtraction,

which can get them anywhere.

Now, a few people take issue

with the equivocation

on the word "stealing".

These people say that

"causing a chain reorganization" is different

from "direct theft".

Because during reorgs

miners can only "steal" BTC

from txns that they themselves have made.

(!) AH

But that isn't true.

If they wanted,

miners could capture

all of the value of the txn.

They just need to make a deal

with someone somewhere

in the txn-creation process.

Slide 13

They make two paths,

controlled by different sides

of the txn.

If neither side surrenders,

the money is trapped in limbo,

forever;

if someone surrenders,

then they get a little "crumb"

instead of nothing

-- the person who did not surrender, gets nothing.

But there are two untrusted competitors

who will otherwise get nothing.

So...

The Upper Path is

"Hey, Mrs. A,

make a new 'first txn'

that gives us all of B's money,

and we'll cut you in."

And the Lower Path is

"Mr. B, you make a 'second txn'

off the first one,

giving us most of your money,

and in exchange

we'll let you keep a little of it

instead of nothing".

No actual communication

or interaction is required,

of course.

Miner would just announce this policy,

and both users would get nothing

until they figured it out.

Similarly, with LN,

you do the same thing

just with the "justice delta".

Although it is a little better,

because the attack is more awkward.

You wait for LN software to be released,

and figure out how to identify justice txns.

And that must be public, if LN is to be useful.

miners can cut deals with their friends,

(or anyone)

by giving them the opportunity to

get a few extra crumbs for themselves

if they agree to steal from a channel

and divert the lion's share

of the profits [to the miners].

Slide 11

Ok,

here's the thing,

folks:

51% miners "can" always steal BTC.

Because they define

the contents of the chain.

SCs do invoke

this assumption

(just as everything does)

but SCs do not change it.

Same security assumption.

---

Now,

before I go on

to my new thing,

I have another observation,

by way of objection.

It is this:

while critics have obsessed

in excruciating detail

over the possible effects

of sidechains on mainchains,

these same critics have

rather suspiciously,

neglected the effect

of \*Altcoins\* on mainchain miners.

Slide 16

Many people in Core development

endorse a theory,

that a small block size

will lead to high fee revenues,

and that this is good

for motivating hashrate security without inflation.

(And I'm not trying to start

anything with this, I'm quoting it

because its famous.)

figure: R1 (large square) > R2 (flat rectangle) on supply demand curves .

Both theory,

and recent empirical evidence

suggest that high fees merely

stimulate the use of Altcoins.

figure: three historical graphs ;; txn fees (top); Bitcoin txns (middle); cryptocoin caps; -- set index 100, log scale, so you can see them all independent of their different units.

I didn't put

a lot here

because I didn't think

that the point was in dispute.

I think it is

commonly accepted that

over the past 2 years,

fees have gone up

and \*some\* users

have stopped transacting

altogether, or are using

Altcoins.

And Lightning is irrelevant

in this example,

because once it is invented

all of the Altcoins

will also have it,

so this same effect will just

repeat itself.

---

Slide

So, there's a contradiction here.

It is admitted,

that fee revenues are important

(for instance that if fees are insufficient in magnitude, then inflation may be required).

Slide

And it is admitted

that supply affects FR.

But demand for blockspace

has been de-emphasized.

But it actually has

a central place,

in this analysis.

Ok watch carefully,

R1 > R2.

Slide

LN is not the only thing

that is irrelevant.

Altcoins can mimic

Bitcoin's security features,

and can even have larger blocksizes

but also \*cheaper\* full nodes.

Because Altcoiners can just

spin up

a completely new chain

every 6 months.

In a world with no sidechains,

whenever

fees on BTC

rise

above \*anything higher than the lowest possible value\*,

then all of the 'payment users' will

start using Altcoins.

These txn fees will \*not\* go to Bitcoin,

so the reverse of what is claimed is true.

In other words,

--absent sidechains,--

the block size limit

makes it more likely,

not less,

that we will eventually need inflation

to pay for hashrate security.

OK - now my new thing.

It is related to sidechains

but I think also of

independent interest.

Slide 13

Bitcoiners sometimes disagree.

Not just about blocksizes!

It is well known that

Bitcoin is a \*consensus\* system.

Everyone must agree.

But \*about what\* are we agreeing?

I think its actually kind of

a complicated question.

I mean

Bitcoin is tolerant

of \*some\* differences,

like in diet.

---

So which differences are tolerable,

and which are intolerable?

Slide 14

It is said that:

you aren't a real Bitcoin user

unless you run your own node.

But this begs the question:

a full node of what?

...certainly not a full node of Litecoin.

How do we tell "a full node"

from

"NOT a full node"?

Slide 15

A superficial answer

to this question is,

that full nodes are

whatever the latest release of Bitcoin Core is.

Which is another way of saying:

That a full node is always

"Whatever Wladimir says" a full node is.

Of course, we all know this can't be right.

But let me quickly sketch out an explanation

for why it isn't right, anyway.

But that would mean:

You aren't a real Bitcoin user

unless your computer does

whatever Wladimir tells it do to.

An inescapable "Wladimir dictatorship".

Even more problematically,

Wladimir might change his mind at any time,

and since I deliberately used the phrase

"latest release",

you're on the hook for whatever Wladimir

thinks should be in consensus today,

i.e. right this very minute.

So not only might Wladimir

make a mistake

-- one that we cannot recover from.

But he also might contradict himself,

in which case the newest Wladimir

version would trump everything.

And that would imply

that we cannot determine anything

independent of him.

This contradicts Bitcoin completely.

Similarly, if you substitute out,

"the Core Developers", (instead of Wladimir),

then you'd have the same problems:

No recovery from mistakes.

Need to determine latest consensus rules.

No independent existence.

And of course

that substitution

is much worse because,

it introduces new (horrible) problems:

How do we know if someone is or is not a Core Developer?

(At least we know who Wladimir is, and what he decided.)

So what defines a full node?

Slide 16

One way of dodging the question

is to say that

the protocol never changes.

In other words, you say that:

It was created by Satoshi in a 100% fixed state.

No revisions of any kind are needed.

Any "mistakes" in the protocol

should remain there forever.

Or else, it is claimed that no

objective basis possibly exists

for classifying any particular "quirk" as a mistake.

Thus, there is no Meta-Consensus problem.

But this position is hard to defend:

Slide

1. Clear Errors -- philosophical meta-consensus would have to admit these mistakes in forever.

2. Protocol can be unilaterally changed via miners (MASF, UASF) -- then, payments made to you, might go "through" these "new txns".

So, imagine that I have not upgraded

to support SegWit

Kevin wants to send me money,

I tell him not to use a SegWit address,

and he doesn't,

but he spends one of his SegWit outputs.

3. Extremely Pessimistic -- Bitcoin can never improve, ever.

4. Stimulates creation of Altcoins / Hard Forks

As it should, really

because we should always

use the best ideas.

So this really isn't

a "Static Protocol" Position.

Instead,

it just says that

all protocol improvements

should take the form

of Altcoins.

Which I think is disastrous.

----

So this is in

kind of a strange position.

1. can't stay still

2. need to use same rules as everyone else

3. protocol itself doesn't learn those rules

(the new rules are created ex nihilo -- out of nothing)

But of course

we do try

to have it both ways.

----

Slide 17

Obviously, the clever trick

is the \*soft fork\*,

which allows the protocol

to be compatible with

improvements that haven't

even been invented yet.

But how are we doing this??

It seems like magic.

And I do like it a lot.

However, there is something

interesting about the SF.

And it comes with

a cool problem.

Side 18

Check out this diagram

I made.

Two incompatible SFs at once.

..is a hard fork.

In fact, every SF is

a HF of every

incompatible alternative SF

that could have been installed there.

Therefore, we notice

some crucial aspects of a SF.

And I think these are

often overlooked:

Slide 30

Read beginning and ending.

So, there are two aspects:

1. Some part of the

consensus system is

explicitly pre-designated

(designated in advance)

as \*ignorable\*.

Users all agree

not to care

about that zone.

2. [ just as crucially ],

users pre-agree that

they should \*never\* use

these OP Codes,

unless they're certain

that everyone else

is using them

the same way.

Slide 31

Some kind of

exogenous authoritative force ---> "gavel" icon!

designates these parts

as ignorable first,

then later

some exogenous authoritative force

decides what

the meta-consensus should be.

Let me give you

some examples

of what I mean.

Slide 32

Read slide.

This is done

by taking one of these

and causing it to

switch from

"always succeeding"

(which is the default,)

to "failing unless New Rules are very precisely followed".

I think its notable that

the addition of these

codes was technically a hard fork.

I think this holds for

all of the future-proofing

in general.

Satoshi built in

a version number

for transactions,

and for blocks.

We pre-agree

to ignore version numbers

that are "too high".

( Higher than those

that we understand.)

We assume everything

we don't understand

is valid.

And we wouldn't

\*construct\* such txns,

unless we knew that we

were doing so in the same

way as everyone else.

Slide 33

Ok, but here's the problem

with the soft fork

that I noticed.

Read Slide

And you can summarize it

with one question:

--> "What's up for grabs?"

In other words,

"Which aspects

of the existing protocol

are the ones

that have been

pre-designated as ignorable?"

Table

( Story about my wallet

being held hostage

by the s-value upgrade

could have been obfuscated.

Read source? Then Bitcoin

is not for everyone, it is only

very small class of specialists. )

( Mircea -- only addresses

that start with a 1 are real. )

----

In fact,

we also have the

converse problem:

Not just "what's up for grabs?"

But also: did I \*agree\* with

what you put there instead?

For example, say:

1. I haven't upgraded

to SegWit, and you have.

2. Someone sends you

money using SegWit

3. Then,

in the same block,

you send me those coins

(so to speak),

using a legacy non-SegWit txn.

Now it has, sortof,

become mandatory

for me, after all.

And many SFs

are controversial

because of their impact on

node costs.

An example of this is

the mandatory extension block.

A lot of people hate it,

even though it is theoretically

opt-in.

Adam Back had a scheme,

early in the Scaling Wars,

for making an ext-block

one-way and keeping it mandatory.

( In fact, today,

is impossible to demonstrate

that Bitcoin miners haven't already

SF-ed to add a 10 GB

mandatory extension block.

One that they just

don't tell anyone about. )

Slide 23

-So my original question,

"a full node \*of what\*"?

What is a full node?

It actually seems to be

quite arbitrary.

Image: software versions as squares.

(each slot, is a protocol)

Slide 23b

--> software versions as themselves a blockchain

( but one that we cannot verify --

it would be interesting if we actually timestamped

all protocol changes into the blockchain itself --

but actually I think that that would be

an infinite regress )

Slide 24 (?)

Conclusion Slide

\* Sidechains \*are\* a layer-2.

(There is no basis for preventing users

from using them, other than tyranny. )

\* Sidechains use the same security assumptions.

(They may have a different security model,

but the 51% attack is a weakness shared by all

blockchain technologies.)

\* In fact, \*lack of sidechains\* is the real threat,

because unlike sidechains, Altcoins do affect

Bitcoin's mainchain miners. Altcoins are the real culprit.

\* Soft fork has “zones” (of “ignorable” and “defined”),

the boundary and range of these zones

is not clearly defined,

which leads to conflict.

Call to Action

1. Reject sidechain FUD, remember user-soverignty (if user has a right to buy an Altcoin, then they have the right to use a sidechain)

2. Check out the project ;; soft fork on the latest Core code ;; testnet ;; diff 93 pages

Slide 13

But I think that sidechains help.

(!) Yes. You all knew it was

going to tie back to sidechains

somehow.

(Sidechains,

for those of you who have been living under a rock

are a response to Altcoins --

-- they let you send your Bitcoin to a completely different

piece of software).

For example the RSK software that emulates Ethereum.

And when I use the term sidechain,

I refer always to \*optional\* sidechains.

...

## Q & A

### Why is this moving so slow?

Use "5 Qs" answer #2.

### Has the code been peer reviewed?

Yes a lot. In fact it has probably had more peer review than any soft fork ever.

\* Posted in Nov 2015, with a 5, "reddit peer review" including from Greg Maxwell.

\* \* Four hour Youtube Presentation in June 2016 to respond to that.

\* \* And then I gave another talk about SC risks.

\* Adam Back put together a little drivechain summit that had Blockstream guys + RSK guys + Zooko and like a few other people. And that had an email thread.

\* Then I presented at Scaling III, and afterward we had sessions with Sergio who had done a parallel implmentation; and Matt Corallo and Sipa --> blind merged mining , that was January 2017.

\* Construct --> Around/during Consensus 2017 there were all of the bitcoin-dev mailing list discussions.

...there has been lots of ongoing peer review.

\* Satoshi Roundtable IV -- Feburary of this year, we had a big "tech experts room", we disussed it for like four hours.

\* I can't remember what happened to the BIPs, but one has a number 301.

\* Wayne at Tierion hired Mark Friedenbach to do some code and architecture review which he is --more than halfway through.

But the thing is that an opt-in soft fork like this doesn't really need peer review, because you can just shut Drivechain I off by a soft fork, and then soft fork in Drivechain II, although obviously that is embarassing and not ideal.

And no one has ever found a bug in the code, because ...you know what the code is perfect and no one here is smart enough to find any bugs in the code ... and definitely not smart enough to publish those bugs in a very humiliating and public way.

### Why is it false that a block size is needed for a fee market?

(( It is a similar format to that of the second misconception -- a situation where miners can add and subtract something. So they can always make a block's size smaller, by including fewer txns, and, unless they hit a node-enforced block size limit, they can always include the marginal txn, and make the block size larger. ))

Miners can estimate (very easily in my opinion) what the optimal block size is, and enforce (amonst themselves) that blocks be roughly around that size.

Appendix

-----------

The problem is

compounded tremendously

when you consider that

the soft fork doesn't

only maintain

a consistent UTXO set.

It also prevents

maintenance fees

from getting too high.

By maintenance fees,

I mean:

the "cost of starting up

a new full node",

which I also call "decentralization".

But, if the theory were false,

then there would be no basis for preventing a user from

using a sidechain,

other than tyranny.

Its like East Germany, right?

...the wall is not to keep barbarians out,

its to keep you in.

So it's an important question -- which way are the walls facing.

Slide 20b

--> So soft forks actually require

a "hard" setup.

Nonetheless, these setups are "safe"

because users can ignore

any and all soft forks,

and take as long as they like

to upgrade,

even forever.

It helps us with our question:

Bitcoiners don't have

meta-consensus

on which software to run

but DO have it that:

that consensus should be about

\*who owns the Bitcoins\*

( or really: what owns them )

and nothing else.

So diet and favorite color are out,

and "Who owns what?" is in.

----

And I think the soft fork is

--> Soft forks have automatic error-correction.

As a direct result of ignore-ability,

softfork-upgrades will automatically

recover from mistakes.

This is because

users can choose

not to use

a broken new feature,

-- this conceptually returns it

to its [original] "ignorable" state.

Wow -- I sometimes feel that the

soft fork is

as interesting as Bitcoin itself.

Its really remarkable as an

institution for making progress.

----

Ah but don't you remember,

what I just brought up,

the idea of all of these

payments-to-you

going through txns that you

don't understand

the "loudness" of the fork

(or the "volume").

That might be fine though.

We forgot something, though,

not just "Who owns what?"

but also, making sure it is

easy to run a full node.

Ok,

1. Who owns what?

2. Keep the cost of full node down.

A

That second one

And compounding this:

Moreover, there's no recourse,

if there's a SF that you don't like.

And, two groups of people can

SF unilaterally:

Miners w/ MASF

Users w/ UASF.

So, Bitcoin seems to

evolve,

by trial-and-error,

in an unpredictable

and uncontrollable way.

So I'd like

to tell people

that they need

to run their own full node.

But honestly I am

having a little bit

of trouble figuring out

exactly what that means

or what it really implies.

Sidechains do offer a

solution to this problem.

in addition to resolving

the scalability debate

and destroying Scamcoins.

So really

I actually think that

it has no answer,

and is unanswerable.

Because ???

\* Secret rules

\* Unilateral rules

\* Arbitrary "exogenous process"

-- that must be ordered

It's own chain!

~~ embrace the ambiguity,

help the situation ~~

But this problem

is sidestepped completely

if development moves

to Layer-2 with both

LN and Sidechains.

--

@ truthcoin

paul@tierion.com