Anarchapulco -- Feb 2024-- Paul Sztorc

~rapport~

Hello, thanks for having me. And happy Valentine's Day, for what it's worth.

~Agenda~

Here's what I have planned – 30 minute talk , plus 10 minutes of Q&A. -- Brief introduction … then, what is the title about, what does it mean … what is the sidechain … how you guys can use it, today (if you want) this is freely available software that already exists, and is under active development … and finally how you can help me, -- you know—if you agree with what I have to say. Of course.

So that's the talk, I hope you like it – if you don't like it… now's your chance to escape!

~About Me~ Long ago, I was a statistician in the Yale University Economics Department. Then in 2013/2014 I became a Bitcoin Researcher and started this blog, truthcoin.info. Where I've written a ton about Bitcoin.

~slide~ my big break , so to speak, was in Dec 2014 when Adam Back linked to my blog. There it is – this essay became the famous "Nothing is Cheaper than Proof of Work" essay, from 2015, which is one of the earliest essays criticizing Proof of Stake.

~slide~ Since then, I wrote this P2P oracle thing for Bitcoin, which I presented about here at Anarchapulco in Feb 2019 -- you can read about that BitcoinHivemind.com . That's one of the many important use-cases of sidechains, by the way. Sidechains are enabled on BTC, via BIPs 300 and 301, which I wrote. Last year I raised $3 million dollars to start LayerTwo Labs, to work on this type of technology. -- So that's me.

~Title~

Now --- the title is "Victory, Unity, and Freedom – via sidechains" … but what does that mean?

~slide~

Well, by VICTORY I mean that crypto defeats fiat. , And by CRYPTO I mean : opensource software that protects the user's rights. , And by FIAT I mean : allowing the government, to *create* as much money as they like, *spend* as much money as they like (on whatever they want), take as much money as they like, and destroy as much money as they like.

Now --- [joke], obviously we have some anarchists in the audience, but even if you're not an anarchist, *I*

mean , this is kind of a lot. Why anyone should have this kind of power ? is not really appropriate. I'm honestly surprise that everyone on Earth has been letting them get away with for this long.

But if it's a mistake, then what are we gonna do about it? Cryptocurrency has done very well, but how can we make it win – like really win, like 8 billion people on the planet earth using it , everyday. How are we going to do that?

~slide~

I think Victory = Unity + Freedom , basically . So now I have to define these two.

Unity refers to my belief that *only one coin should win* . For the following reasons: (1) more new coins necessarily implies inflation (which is taking someone's money); (2) more new coins, implies that the existing coins are subject to replacement, which means the old coin will die off – and that's not good. It also means that everyone needs to research all the new coins (which is annoying); (3) having multiple coins is a *contradiction* because it is a regress from money back to barter. So, imagine that each of us had our own currency, that only we used. That is kind of ridiculous --- it is as if each of us spoke our own language.

Money and Language are not *individualistic* , they are *social* – you want to speak a language that your audience can understand, and you want to spend *money* that your trading partner will *accept*. The consensual nature of it, implies some reciprocity. What you prefer, is mostly determined by other people. And vice-versa.

Hence the (4)th reason: network effects. Which language should you learn to speak? Your benefit is highest, if you speak the language *most listeners* understand. It's the same with money – you prefer to carry around, money that the people around you will accept. And you prefer to receive from others, the money you can spend – to them. Your preferences depend on other people. Hence the paradox – if we want to win, you know -- if we want "victory" up there , we'll have to understand that *teamwork* is crucial. So: unity. Teamwork is success.

Now, one final thought on this: the idea that only coin should win, is sometimes referred to as "Maximalism". As in … "laser-eye Bitcoin Maximalism". That is the view that it will be Bitcoin BTC that wins. I used to hold that view - - Now less so. My view today is that the first *sidechain-enabled coin* will win.

Because the third point – freedom, is just as important as the 2nd point (unity). And the sidechain idea is the key to achieving *both*. Because otherwise they would conflict with each other.

~slide~

So what do I mean by freedom?

Well: we need ***competition*** . We need multiple blockchains, and the ability to *make* a new blockchain **easily and efficiently.**

Now, I must stress – this does NOT mean, that there will be 8 billion blockchains. After all, there aren't 8 billion entrepreneurs , or 8 billion corporations. Not everyone should be an entrepreneur. Not everyone is cut out for that. But – we all know – what kind of society is better? One such as Singapore,

where starting a new business requires a single one-page form? Or a society where you need government permits for everything to .. become a barber , or dog walker. (So Massachusetts actually requires a license from the state, so…) Anyways -- the cheaper it is to create a new business, the more competition there is. There mere threat, that someone might start up a new competitor – that is often enough to keep the current businessmen honest. And the reverse is also true: if your job is safe, and you can never be fired or replaced, then you are likely to become pretty lazy. (I mean, it would irrational not become lazy in that scenario.) And who will suffer, from your laziness? Your customers. Conversely, if your customers can go down the street, to the next guy, that keeps you honest.

(read box here)

~Slide~

So in particular, we want:

21 million coins only
Multiple blockchains, run by *different people* who all *hate each other*
The ability to always add *more new blockchains* if we need them.
The ability for *users to always switch* between these as they like, without asking permission … and especially, without asking permission from the developers on the chain they're on.
(That would be like asking the North Korean government for permission to leave North Korea – instead, the coins have to be able to switch at any time, at the touch of a button. Unilaterally.

I have some visual aids to help convey this idea, but before I get to those …

~slide~

… I feel the need to do a small history lesson on the word "sidechain". It was originally from the Blockstream 2014 paper, Enabling Blockchain Innovations with Pegged Sidechains. Unfortunately, by January 2017 they had abandoned this idea completely. They replaced it with the "federated sidechain" – my view is that "federated sidechains" are basically a fraud, it is a lot like saying "dry ocean" or "tall short person" because the defining feature of a blockchain, is that it is Peer-to-Peer. But the defining feature of the so-called "federated sidechains" is that there is a group of fixed people who run everything. They control the state of the chain, they can steal all your money, they collect all the txn fees (instead of the miners).

Meanwhile, I had tried to implement Blockstream's ideas, in code, back in 2015. Which led me to realize that they were mostly doing it wrong. And so I invented and published my own thing here, called "drivechain" – But, perhaps confusingly, I still use the word "sidechain".

Blockstream still uses the word sidechain also. But, after Jan 2017, it was clear that they had something very different in mind for word.

This was very disappointing to me, so after learning about this bad news in 2017, I set out to develop the real P2P sidechains. So in Jan 2017 I made the project site "drivechain.info" . In Feb 2018, I wrote these two BIPs – 300 and 301 . We cloned our first altcoin back in 2020, during covid – the zcash Altcoin. And then in Dec 2022 I created this company, LayerTwo Labs.

So, I'm kind of fighting a doomed battle, over the meaning of the word "sidechain". To me, the federated sidechains are "Fake Sidechains". People call my thing "drivechains". That's fine. When I use the term sidechain, I am talking about a decentralized process, whose rules are enforced by proof of work -- by miners and full nodes. No leader, no hardcoded keys --- no one in a special privileged position – like an unfireable position (with no competition – that would be ruining the whole thing). What I'm talking about, is a process where everyone is equally vulnerable to being replaced by the process. And fired. … And I'm trying reclaim the OLD idea. The good one.

~Visual Aids~ Okay, here's those visual aids. So, right now, each blockchain has its own coin. No sidechains. But afterwards, there's just the one coin. With different blockchains on top of it.

~slide~ so , no need for the altcoins. So this the unity point. Everything united under one coin.

~slide~ second visual aid . With no sidechains, Bitcoin is kind of like and OLD PHONE here. But with sidechains it becomes a SMARTPHONE and a smartphone, as we all know, can imitate these other devices, you know like a videocamera or a radio.

~slide~ third visual aid. So, again, the world of Altcoins is on the left, and the world of sidechains is on the right. We have clones of the Altcoin software. So the "Bit-Monero" sidechain, in the top right -- it would do whatever the Monero altcoin would do. But there's no XMR, on Bit-Monero. You send BTC to it, and back.

~slide~ Finally, I have this keyboard thing. Same 88 keys, as a piano, but you can produce any sound.

~slide~ Now, obviously in cryptocurrencies there are many scams and a ton of vaporware. So: here's the good news. Quite a lot of people like this idea… You should visit this site for yourself : Layer Two Labs (dot) com (slash) friends. … and we have all of these people … and we have all of their quotes.

… but MORE importantly …

~slide~ we have working software – at releases.drivechain.info now . So, this software works today. We are testing it, improving the UX, we've started to show it to more and more people, such as yourselves. It works today.

(I feel like I'm always saying this – but don't download it now, because we have a new version coming out that's much better, probably tomorrow even. Always new versions are coming out. So don't download it yet.) … but it is there. This is not vaporware.

~slide~ Here is a list of sidechains we have already built. And that we are building now. We've already cloned zCash , a great privacy coin, and Ethereum, the #2 coin.

(wing it)

~miners~ Everyone benefits from the sidechain idea. I'm going to explain it from the miner's point of view, because I think it makes the value proposition a little more concrete. It also helps you in the audience understand what has to happen, in order for us to … use this idea.

…

The goals of BIP 300 , are that every transaction in the world, be a Bitcoin transaction ; and for

each of these to contribute to miner revenues. We want Victory -- Planet Bitcoin. But the other goal is Freedom -- different networks , competition – to accommodate different people. We want competition among developers. We want developers to work hard, for the user. The harder they work for the user → that means more users, more transactions fees, more Bitcoin adoption.

~slide~ so –making every transaction in the world a Bitcoin txn, that is Bip300. And 301 is pulling

all of the revenue from those networks, to miners.

~slide~ So – another image here. This is the goal. This is a website cryptofees.info , by the way, if you didn't know. It keeps track of all the fees on all the different networks. Anyway, we want to convert Alt projects to Bitcoin projects, and convert the L2 fees to L1 fees. So, ~slide~ there you go. Bip300 in green, converting Ethereum in Bit-Ethereum. And the in blue, pulling all the fees into L1 Bitcoin.

~slide~ And we aren't limited to the Altcoin networks exist. We can use this technique on any network. Including some new ones that we build from scratch, TRON, whatever. Since earth had 1.1 trillion txns last year – about half of those were card transactions. If you were to just take ten cents from each other those, it would be $100 B dollars. Not bad sinice usually mining revenues are merely 5-10 billion. That's just some basic envelope math for you – but if you go down to ten cents, it means that you are cheaper than most payment networks today, and also a competitor can only undercut you by nine cents, at most. Which probably most end users don't care about nine cents.

It is also just easier to chase revenues than it is to cut costs, at least in my opinion. Miners get two for one – more users is more transaction fees, but it is also more Bitcoin adoption and a higher price.

Also, users hate high L1 fee-rates, so it is easier to get more users at a lower feerate, than it is to increase the fee-rate. People hate the high feerates.

~slide~ now this is important, because BIPs 300/301 can be activated by the miners alone. So that's the ask.

~slides~ Finally, some thoughts on why I think is – really, --- definitely, the way to go.

Commanding heights, Batting Cleanup, and Culture

~slide~ Commanding Heights, this is an idea from warfare. Like if you capture a hill, then the enemy has to surrender. Interestingly this phrase was also used by Marxists to describe parts of the economy they wanted to control first-- ugh yuck, we don't want that. It was also a book, where the author Daniel Yergin used it ironically to describe the triumph of free markets … there's now a 6-hour PBS documentary that you can now find on youtube. Anyway – what I mean is – the winning victorious coin, needs to excel on these three dimensions , *relative to its rivals*. Capture these, first, then you win the game.

(read slide)

~slide~

Ok batting cleanup – Bip300 (ie sidechains) also solves these problems, as a kind of side-effect
(read slide)

~culture~
Ok, culture – my view on culture is that it is often a parasite. It's like peer pressure – people feel compelled to conform, to fit in.

It's why I like coming to Anarchapulco because there are so many wierdos here. Non-conformists unite!

Anyway, the point of this slide is that BTC culture has become kind of defective, and is killing the project. Not enough ***competition*** of ideas. And so now we have bad ideas in BTC. But the sidechain would fix that.

~how to help~ Ok how to help:

The best way is , to learn and spread the word.