~Title~

Ok – hello.

~Agenda~

I am going to talk about something called "CUSF" – which is the solution to our current problems. So – you're welcome. But it is going to take a little while -- to give the whole explanation, for ***why*** it is the solution to all our problems, and I only have 30 minutes, so:

- 15 minutes background on the problem, about me, the context - -what I think is important
- 5 minutes about CUSF and how it solves our problems
- Q&A – I think Q&A is where the magic happens, -- and I have some pretty audacious things to say in this talk, so its only fair that people be able to examine them.

~My History~

I spoke at all 3 of the first Scaling conferences, and I was on the program committee for the 4th.

Back in Dec 2013, I invented this P2P oracle / prediction market blockchain called Truthcoin, which was supposed to be a sidechain L2 Bitcoin , back then – I quickly re-named it BitcoinHivemind.com , because people thought it was an Altcoin . You can still go to that site and check it out. This project basically became PolyMarket which became very famous this month . If Blockstream had delivered on their mission, back in 2014 to give us peer to peer sidechains, then this would have been a bitcoin sidechain, a long time ago – like more than 10 years ago – and miners would have gotten a cut of those transaction fees. This was billion in transaction volume, last month. That's important.

Since Blockstream failed to deliver the sidechain technology, I did it myself – it began as this essay "Measuring Decentralization" in Sept 2015, and then became the "Drivechain" blog post in Nov 2015. This became Bip300 today – and Bip300 could give us planetary scale & zCash privacy, and improve mining decentralization. As I'm going to explain.

Furthermore -- I did a presentation in June 2016 called "sidechain privatization" which basically anticipated MEV, This later became an invention called "Blind Merged Mining" in Jan 2017, which later became Bip301 → today it would be known as "'proposer-builder separation". And what does it do? It automatically converts all L2 block value – including (txn fees, indirect value, DEX arbitrage, whatever) all that value into L1 transaction fees. Miners don't even have to look at what is happening on the L2 – hence the name "blind". [3:20]

Plus – more stuff. Ok, so that is me.

~Motivation/Endgame~

Ok -- this is the endgame for Bitcoin as I see it. These circles are to scale – the left circle is total transaction fees paid to miners in 2022. The next one over, is fees in 2023 – the ordinals year. The third circle is all transaction fees paid by all Altcoins (2022). And the big circle is the value of all txn fees paid on Earth (2022). Ok so – this my estimation.

Now – how did I get this number? 6.4 trillion txns/year , times $0.10 per txn. – So, I looked at statistics for credit card companies, across different years, I looked at WeChatPay statistics, The Federal Reserve has a study of payments volume, that they do every year. – The details are in this blog post – but basically I eyeballed it. 6.4 trillion transactions in 2024. And *ten cents* per transaction – because that's much lower, than the transaction fees people pay today , so they'd happily switch – but once you get to ten cents, a new network can only undercut the price by about nine cents, which isn't very much. That leaves $640 billion dollars. Ok you can look at the details if you want. Oh and – this value appears to be growing at a rate of 6.2% per year – in other words, the area of this circle doubles every 11-12 years.

~Mined vs NonMined L2s~

Ok - the first thing, is to ask a very important question: *if Bitcoin took over the world, who would get this money*?

The current intellectual climate, is pushing non-mined L2s. -- -- The Lightning Network – ARK – Rollups -- Liquid. All of these L2s are *not mined* L2s – the txn fees *do not go* to miners, instead they go to someone else -- the lightning node , or the LSP -- or the ARK-SP -- or the sequencer (the rollup sequencer). The money goes to someone else. [[6:30]]

Now, first of all -- this is kind of rude to the miners. But it's way worse than that.

~Instability~

It produces a *horrendously unstable* situation, that will end in: 1) conflict (between L1 and L2), 2) huge incentives for miner-centralization, and then eventually, 3) *vertical integration* between the L2s and the L1 miners, and this vertical integration will 4) utterly obliterate the entire L2 security model, in the first place – which means that all the code [[these people]] plan to write, is just a waste of time, the L2 will end up fully custodial , possibly even miner-custodial. The value will all become MEV, in fact.

Ok – let me explain a little more about that. I mean sure, the miners get a small circle, but what can they do about it?

~Miners vs L2s Honesty Hashrate Majority Assumption (That No One Talks About)~

Unfortunately: everything. Well , *every L2* is vulnerable to 51% attack , by L1 miners. For example, the Lightning Network requires an L1 txn to join the network, and one to leave the network, *and* the LN only works at all, if you can broadcast “justice transactions” to L1 whenever you want. And of course, 51% miners could censor these txns.

If do not believe me – here is Rene Pickahardt – author of the book Mastering Lightning – he is saying exactly what I am saying, here. It’s the same for BitVM – BitVM requires that the miners NOT censor – their version of the justice txn, which basically a transaction proving that someone broke the L2s rules . If L1 miners censor these, then the security model of BitVM no longer applies. No matter what the L2 is, the L1 miners can block the *entrance* and the *exit*.

~back to circle~

So, if we return to our example, where you have like “Foundry LSP” or “AntPool LSP” , on one hand, – versus -- lightning nodes that are not backed by giant amounts of hashrate – then it would be completely understandable for *users* to get nervous using non-mined LSPs , because they would not be secure , the HTLC would do nothing -- eventually those LSP would go out of business, eventually everyone would use a miner LSP – all of HTLC stuff would be superfluous. Ironically, it is *because* the L2 was so *successful* that the miners would want it. The original Lightning security model *wouldn’t even apply* in this case. All of this L2 value , would become MEV – since -- running a Lightning Service Provider, would now become a complicated and mandatory thing, that every viable miner must do. And they would have a monopoly, as well – because you can’t start a new lightning company now , or a new mining pool -- its like Super-MEV. [[10 : 33]]

~conclusion~

Ironically, at that point, the only way to undo the MEV, would be to create a mined L2, and hope that people switch it. So, even if these had *succeeded*, we would end up, wishing that they had failed.

In other words, the NonMined L2s are not going to work. Of course, they may “work” in the superficial sense, of the software not breaking. But they will never be big – they will never be a big success. They will never be this huge circle.

Because as soon as they are, miners will think – “why am I getting this tiny circle”, whereas “the LSP is getting this huge circle”. And then, the miners will think: why don’t we just start our own mining LSP. – Foundry LSP -- And then – it will be, on one hand, *LSPs backed by huge miners* , vs LSP that are not backed by any miners. Which is a battle where one side doesn’t have any bullets.

~My Proposal for Mined L2s~

So instead, here is my proposal for Mined L2s. (Which I call 13-13)

The details are in two blog posts of mine – here is the first.

The proposal is L1 small Blocksize at the top – and then 13 separate L2s distributed amongst users geographically -- each released one-at-a-time, as the previous ones fill up, they start with –what is the equivalent of -- a 13 MB Blocksize , which grows over time for each of them. ~ table~ This allows them to reach planetary scale, by the year 2030. That is 9.8 trillion transactions per year, so this is the schedule. || it is much better than Lightning in the following ways: it has no channels, no interactivity requirements, no liquidity problems, you can onboard people directly to L2 (without using L1 bytes), payments never fail. – And , of course, 100% of the fees are passed down to miners. Instead of 0%.

It also improves miner centralization, by allowing smaller & faster cashouts, from pools to hashers.

And, on top of that, it does NOT require, any changes to Bitcoin Core – at all – but it does require CUSF – which I promise I am getting to.

~Screenshot~

And, if all of that weren't good enough, this software already exists , today – here it is! It even has a little GUI. – Bitcoin Core is in the bottom left – that's L1 – the L2 is in the top right. This is the CUSF version, in fact. What is CUSF? – well, I'm so glad you asked… I'm getting to it.

~CUSF~

Ok – CUSF stands for "Core Untouched Soft Fork" – , it threads the needle between two deadly roadblocks:

~Ossification Table~

Ok these numbers are from BitMex Research – but I put them in this table. This is a table of soft forks, in Bitcoin's history. As you can see, we used to do ~ one every two years, or so. Now we do , basically zero. I also look up the time, it took – from 1st mailing list suggestion, to code, and then finally to activation. SegWit took 20 months, but Taproot took 46 months. So you see this is just winding down.

This -- -- is the miner's neglect. Miners think : "oh, soft forks are just some tech thing, it doesn't really affect me – we'll just wait until everyone agrees, and then tells us what to do" . Wrong. Miners have the most illiquid position – miners stand to gain/lose the most, from Bitcoin's success or failure. Miners are huge holders of Bitcoin.

2nd problem is : you can't leave.

Number One -- The Bitcoin Core process isn't working anymore – for soft forks. Just, the empirical reality. – Number Two – No one wants to leave Bitcoin Core. – It is too risky, being disconnecting from the real network, who will support the new client? Who will deal with the CVEs? When push comes to shove, there really is no way to compete with Bitcoin Core.

So, the solution is to *keep Bitcoin Core, unchanged,* and release a second piece of software, that manages the soft fork only. **So, after Bitcoin Core scans a block, the OP CAT activator scans the block again, and if there's any OPCAT-rulebreaking, it tells Bitcoin Core to reject the block.**

Soft forks faster, safer, easier to understand.

~paper~

So, here's my big paper about it. I stashed it at "Bip300cusf (dot) com".

~software~

And , we also have software – already. There it is. We can activate any soft fork this way – but the software on the website now will activate OP Cat, or Bip300. .. And you can fork our software – for that -- and add CTV or APO or whatever.

~re-explain~

Ok I am going to explain it again.

[read right bullets]

~proposal~

My proposal is:

- Miners run the Bip300 CUSF activator ;; (meanwhile Bitcoin Core continues to do nothing – they're very good at that) …… [read slide] ……

Miners could theoretically do this very soon, if they wanted – but the smart thing, of course, would be to think about it very carefully, before doing anything.

But that is what I think would fix all of Bitcoin's problems.

Finally, the alternative….

~Alternative~

… to me , the alternative plan seems NOT very good.

~tables~

More about CUSF. I have here a big table, with all the benefits and differences of CUSF vs other soft fork activation methods.

there are too many veto points , for example, Ava Chow has said [quote] if a proposal is even slightly controversial, we will just never discuss it [close quote] – but anyone can make fake controversy about anything -- the layperson doesn't understand the soft fork – people think it is a change (even though it isn't a change because the old network survives). So – Bitcoin Core doesn't work anymore, for soft forks. And in fact, plenty of people – Francis Pouliot included, think that no soft fork should even come from Bitcoin Core – instead they say it should come from elsewhere and Core should later update to be compatible with it. So, if you wanted that, then you are getting your wish.

2) Roadblock #2 -- NO one wants to switch away from Bitcoin Core – to something else. The existing thing doesn't work – and we can't switch to something else.

CUSF

my proposal is: -- miners keep running Bitcoin Core – they add to that, a 2nd thing they run – CUSF Activator –

~Focus~

My proposal is going to be:

I am a software developer – we'll see some software at the end– but really my background is in economics.

I have this focus on *happy users* → which translates to *paying fees*

And I am much more interested in situations where *everyone is getting rich together* , vs some kind of unbreakable "cryptographic security". Prefer something where the miners cannot interfere, but I am more interested in situations where the last thing miners would ever want to do, is interference, because they are making so much money. They see it more like a prison – where we have to plug all the gaps, and prevent people from every escaping – and in contrast I see it a little more like a restaurant – where people want different things and everyone is getting what they want. This different model allows me to push the envelope significantly further than anyone else – and I think it also dodges a lot of bullets, too as I will explain.

I still haven't explained it yet – but I will. – We're almost there. We're getting closer. --- There really is a lot of context I have to explain first. – But this software is real -- you can get it from github, or our releases server. – And this software has fraud proofs, and UTreeXo , Tadge, I threw it in there,– although now I think its kind of overrated because of, data availability problem – so you can't actually have a full node on your phone, because a full node is serving the historical blockchain to everyone. To regenerate the network. U-tree-XO.

~unilateral exit~

Now I have two comments – "Unilateral Withdrawal" and "When to Soft Fork".

Everyone is in love with this unilateral withdrawal idea – to me it is obvious that it is a complete waste of time. 1st – (as I mentioned) -- 51% hashrate can always "interfere" with the L2 – not unilateral in that way. But more importantly, imagine 8 billion are using the L2 – there's not enough space for 8 billion people on L1. They can't fit on L1 – so there's no such thing. If the L2 is successful, --significantly more users than L1—then it cannot be unilateral exit. Only the people who can fit on L1 can exit. Thirdly, and probably least importantly – if the L1 fee rates rise about the UTXO value – (the value of the UTXO you'd redeem on L1 as part of your so-called unilateral exit) – if the L1 fee rates rise above that, then theres no way of you getting back to L1, without it costing the end user more money than they would actually get. So if L1 is successful, and the fee-rates are high, then unilateral exit will be impossible. All these things depend on what other people do – so they are not unilateral at all! It's completely dependent on other people. – I don't know why people think, this criterion means anything, I think it is a complete absurdity. – But hey maybe Q&A – people can straighten me out.

~My History~

Ok here's some things I've done in the past.

This is all necessary, to understand CUSF – because to understand CUSF you must understand me, and what I'm talking about -- and why. And I'm going to say some pretty crazy stuff later, so we have first point out, how ***completely correct*** I have been, in the past, many years before everyone else.

This conference aims to continue the tradition of Scaling Bitcoin Conferences. I spoke at all 3 of the first Scaling conferences, and I was on the program committee for the 4th. And then they started to suck –no offense—but now I'm happy to be back. I hope this conference is a success.

Back in Dec 2013, I invented this P2P oracle / prediction market blockchain, called Truthcoin, which was supposed to be a sidechain of Bitcoin – I quickly re-named it BitcoinHivemind.com . You can still go to that site and check it out. Other people , later turned this into Augur/Gnosis on Ethereum, and eventually today PolyMarket (which is kind of a paired down version, of what I made) -- which recently had billions of dollars in trading volume and took on enormous relevance, in the election this week. If Blockstream had delivered on their mission, back in 2014 to give us peer to peer sidechains, this would have been a bitcoin sidechain, a long time ago – like more than 10 years ago – and miners would have gotten a cut of those transaction fees. That's important.

Since Blockstream failed to deliver the sidechain L2 technology, I went ahead and did it myself – it began as this essay "Measuring Decentralization" in Sept 2015, and became the "Drivechain" blog post in Nov 2015. This became Bip300 today – and Bip300 could give us planetary scale & zCash privacy, and improve mining decentralization. As I am going to explain.

Furthermore -- I did a presentation in June 2016 called "sidechain privatization" which basically anticipated cross-chain MEV, This later became an invention called "Blind Merged Mining" in Jan 2017, which later became Bip301 → today it would be known as "'proposer-builder separation". And what does it do? It automatically converts all L2 block value – including (txn fees, MEV, indirect value, DEX arbitrage, whatever) all that value into L1 transaction fees. Miners don't even have to look at what is happening on the L2 – hence the name "blind". This is used today in Ruben Somsen's Spacechains, and a couple other things. People still talk about MEV today, even though I solved this problem long ago.

I did also have an essay called "The Win-Win Blocksize solution", from July 2015, this later became known as Fork Futures. The essay from Steve Lee / Ren (from earlier today), they mention this idea several times in their paper on soft fork governance.

I wrote something called "BitAssets" which later became Anduro's Coordinate, if that had been online, the ordinals phenomenon would have happened on a Bitcoin L2 and not on the base layer.

Ok, so that is me.

My "The Win-Win Blocksize solution", from July 2015, this later became known as Fork Futures. The essay from Steve Lee / Ren (from earlier today), they mention this idea several times in their paper on soft fork governance.

I wrote something called "BitAssets" which later became Anduro's Coordinate, the idea for this, is to have the ordinals phenomenon on a Bitcoin L2 and not on the base layer.

~When to Soft Fork~

Ok – I read this paper – and there's this section about "motivation to adopt" the soft fork. – which is fine – but I have a completely different point of view.

~my view~

My view is that it is life or death. --- We aren't like tweaking some knobs, here-and-there. Either we are going full throttle, in favor of innovation and adoption – or someone else will. And that person, will probably succeed – and if they succeed, then we fail , and the project is destroyed. --- --- So the price is at all-time-high which is great – of course – but really it just attracts more attention from other people. It blazes the trail for someone to follow us – and they're going to be thinking , you know – how can I do Bitcoin, but better. Until we have more actual adoption, more transaction fees -- we are vulnerable. That's my point of view. – But I was thinking why is my view so different?

~Innovation/Adoption~

My view is that innovation and adoption will make or break BTC. And the thing about innovation is – its very unpredictable. For everyone in this room – there was a day , ***before*** you had heard of Bitcoin. And then you heard about Bitcoin and you were like, wow amazing. So it could always happen again. I view ***adoption*** as just one particular kind of innovation. Someone will figure out, how to make crypto popular – the PolyMarket idea I mentioned , at the beginning of the talk , for example.

But what really concerns me is this…

But --- final idea…

~heads~

This is an excerpt from a book – I don't know if I have time to read it. Basically, the idea is – there was this prosperous island, that made these statues → and then the society started to have problems → so they responded to the crisis by increasing statue production by like 50x → this caused the society to totally collapse, there was cannibalism, death, everyone died → but when they all died, they were making more statues than ever. They cut down all these trees, that they needed for food – to make more statues. So – they had the wrong idea, which they pursued ever more vigorously. Until they all died basically.