~title slide ~

Okay, hello. I've been invited to speak about Bip300 … which is one of my ideas for taking Bitcoin to the next level. …

~Overview~

Bip300 proposes these new layer2s, that some call "sidechains". Sidechains are a response to the threat of Altcoins, but they're also a response to the desire of Bitcoiners for creativity, and innovation – -- you know: the desire to try new things without asking for anyone's permission. How can we let everyone try the ideas that *they* like? And how do I keep other people's *bad* ideas away from me? So here you see we have the world of Altcoins on the left, but then, the revenge of Bip300 on the right. We have copied Ethereum and Monero into our own projects that respect the 21M coin limit of BTC. No inflation.

~Conversation with Altcoiner~

Ideally, with Bip300, if some annoying person asks "Sure Bitcoin seems great, but can it do .... smart_contracts, DeFI, zk-snarks, blah blah, you just say "Yes, Bitcoin can do that – see Bip300".

~fringe~ Similarly, if some innovator dreams up a crazy idea, "Hey I can improve Bitcoin, it only needs my new idea … larger blocksizes, Turing Completeness, KYC-miner-coins?" Then: similarly, *they* now *can do that* without anyone's permission. They just don't do it on Bitcoin base layer, they do it on a Bip300 sidechain.

So: that's the goal – FREEDOM. Developers can write whatever code they want, users can use that code if they like. Everyone gets what they want. But how is it accomplished?

~3aspects overview slide~ small list ~3screenshots to the right~

I will break the idea down, into three aspects. These are: Full Autonomy ; Protect the Base Layer ; and Improve Miner Incentives.

Before continuing, however, I did want to mention, that this project is *not vaporware*. The code is open source (on Github, right now!), there's downloads with a GUI (we have Windows/Mac versions now), and there's even a YouTube video of me, using Bip300 on testnet, to copy the zCash Altcoin. So the software is very use-able, you can download it right now.

Ok now back to these three aspects.

~1~ Aspect number one: full autonomy. Each new Bip300 sidechain is its own 'app' and you can change the sidechain software however you like. It's just like making a new iPhone app: each "app" has its own development team, the software they write can have any validation rules, (!) or no validation rules.

But, for example, they could add: zk-snarks, higher Blocksize, turing complete scripts, Taproot, mimblewimble, Monero ring-signatures, whatever you like. Any idea –good or bad— can be done and no one can stop them. It's just like releasing a new iPhone app.

Each project starts with zero Bit-*coins* on them. No coins.

~advance slide~- Coins travel from layer1, *to these* other networks. Users have to voluntarily choose to send *their* BTC over. To your software. Just like a lighting App. (So it's a good comparison). Those purple coins are Altcoins … we don't like those. But next to it is a sidechain that does the exact same thing. So....

~slide~ here you see the coins move over. Two coins to Zap, in the lightning world; and one coin to Bit-ZCash, in the Bip300 world. Still 21 million coins total.

~2 ~

Ok, aspect two – the base layer (ie, Bitcoin Core, ie the mainchain, ie “layer1”) that – your Bitcoin node -- is unaffected by problems on the sidechain. Even under very extreme adversarial conditions where the sidechain experiencing all sorts of chaos, Layer1 is just going to solider on, and ignore all of that. The drama can only go *one way.* So, let me try to explain this.

~advance slide~

Here is a representation of Bitcoin’s blockchain. The squares are block headers, and the trailing rectangles are the list of transactions in each block. (Because blocks aren’t always the same size, of course.) And time is flowing from left to right. You can see across the top I’m going from Dec to April. Normally, of course, there would be tens of thousands of blocks (from Dec to April), that wouldn’t have *FIT on the* slides so there’s only seventeen.

Now, what if there was a sidechain, activated, this whole time? Like a clone of Monero, or something. Well, we’ll put it up…

~advance slide~

Here it is. It has its own blocks, and its own block headers, and its own block chain, from December (on the left) to April (on the right). Now, the idea is … that …

~add in the green hashes~

… Three months of sidechain activity are compressed into one little 64-character string here. And that string is the only thing inserted into Layer1. Ever. So, no matter what Bit-Monero over here is doing, *this* is all that layer1 will see.. ready ?

~…~ This.

Therefore, full nodes (on Layer1, down here in blue); they do not check anything that is happening on the sidechain (where there can be, theoretically, unlimited complexity). The sidechain doesn’t need to be a blockchain, it doesn’t need to be written in c++, it can make all kinds of mistakes. Etc. Bip300 operates entirely off of this one little string (here in green). (!) It does *a lot of logic* to that

little string, and assumptions and engineering, game theory economics, etc. I don't have time to explain all of it. But the point is that Layer1 can't be harmed by Layer2 because it really is ignoring Layer2.

I feel compelled to drive this point even further, so…

~slide~ Here is our software. –Just two more slides to finish this point, with a real-world example-- We are looking all the Bip300 withdrawals, there's only one right now. Which is this little row here.

~slide~ Now, the software says "double-click for details", up here. But for the purposes of this talk, that is misleading. Because what the "double-click" does, is try to find a sidechain node on your computer, with rpc-access, so that it can ask questions about the withdrawal. But if you don't have a sidechain full node (on this computer), then if you "double-click" it will just tell you that it knows absolutely nothing whatsoever. So, this little row here, is the entire Bip300 idea.

~3~ Okay third aspect. This one is only this one slide here. Third aspect is that we want to improve Mining Incentives (Bip301).

This is technically Bip301, now. I separated the two BIPs, to make them easier to read. But I think anyone with a brain who uses Bip300, would use Bip301 also – but you don't have to.

Anyway, with Blind Merged Mining (BIP 301), *miners* don't need to pay attention to Sidechains, at all. So, layer1 *users* already weren't paying attention, now layer1 miners can also ignore Sidechains (if they want). They *still* collect all of the transaction fee-revenues from the sidechain's txn! How? Well, they contract with someone else who is running a sidechain full node, and the miner sells *them* the block-rights, basically.

~slide~ Here's the important part – Miners don't run a sidechain node, but they still get all the money.

Therefore, if miners just do what they normally do, today, and include the txns which pay the highest total fees, then they will automatically mine all sidechain blocks and collect revenue from all the

sidechain transactions. Ultimately, I think this concept could boost fee-revenues by 1000x, if not much more. But I don't have time to tell you about it -- I did write two articles about "Security Budget" that you can look up if you want.

Something I want to mention, is that I gave this talk at Bitcoin2021 in June, using these little numbers over here; (on the right). And yesterday I updated the slide ~advance~. Bitcoin revenues are down, ETH revenues are way up.

Maybe that was unlucky timing, *shrug*. Just something to think about.

~Outline~ Ok, here's the rest of the talk. We already made it more than halfway thought. Now I'm going to talk about the Altcoins we should copy. Then I will discuss two supposed Drawbacks of Bip300. And then it'll be over.

~ Possibilities ~ Ok, so we had *the idea*. Now, the *concrete use-cases*. Here are some Altcoins that I think we should consider ripping-off.

~zcash slide~ Obviously, zCash I mentioned at the beginning. ZCash has transactions where the sender, receiver, and the amount are all private. So then we Bitcoiners have to put up with comparisons like this. Where someone puts something up and says "Bitcoin vs Zcash". If we had Bip300, this infographic wouldn't make any sense at all. In fact all debates about one coin vs another coin would make no sense at all. Which brings me to my related point…

~Monero only~ …there is a darknet market that, in Dec of last year, decided to *only* accept Monero. So that's kind of a slap to the face. If we had Bip300, then there would be no reason for them to accept Monero at all, let alone *exclusively*.

~BitDNS~

BitDNS was an idea proposed on bitcointalk, which later became the Altcoin Namecoin. This thread -where it's proposed- is something that absolutely everyone should look up and read, if they have the time. Lots of cool history here. … Satoshi invents Merged Mining, he coins the term "side chain", he writes about how there will be lots of different chains, all back in 2010. It's really cool.

Anyway, this concept, "BitDNS" is a weird idea, but I think it has tremendous potential. Again, I don't have enough time to talk about it. But I did write a big article ~slide~ in Feburary –"BitNames, there's the url", and I will now give you a ***FEW*** of the images from that article. And you can read the article if you are interested.

~this is someone pretending to be Elon Musk, on Twitter~ ; ~this is the Liberty Reserve website domain_name being seized~ ; ~this is a guy on YouTube who, in the bottom-right, has to list out all of his screennames … and they aren't all identical, his Facebook name is different~ With BitDNS everyone would just have one login, for every service. No one could seize your account, anywhere. And people would always be able to find you.

~BitAssets~ – Ok lets talk about digital assets, now. Erc20/NFTs. They're basically digital baseball cards. Except they are unforgeable and indestructible, and unseizable. Anyways, a lot of people have fun collecting things. Most NFTs are on Ethereum, which is really lame. Because we Bitcoiners started all that, with counterparty and colored coins, etc. If we had Bip300, we could have a whole, special ERC20 chain or something. That would domesticate all of this energy in Bitcoin. Instead of having it compete against Bitcoin.

~prediction markets~ This is one of my other projects, BitcoinHivemind.com, check it out. I designed it to be a sidechain from the very beginning. Here are some screenshots. This software can do a lot of things, but the crowd favorite is 'Futarchy' – where there are futures markets for how well certain leaders would perform, if they were in charge. … This idea is very distressing to bad leaders,

[laugh] , because *WE* can learn about exactly how bad *they* are going to be, *before* we cast a vote for anyone. I think that this is one of the most important ideas in the whole world.

~ Sia~

This is Sia, which is David Vorick's project (who some of you may know). (Decentralized P2P cloud storage, managed and enforced by the blockchain). So, you have a hard drive at home, a lot of that space you aren't using. And you also have a bandwith connection at home, most of that bandwith you also aren't using. With this you rent it out. Sia has been running for 5 years, it's very decentralized – it would keep running if the dev team quit. He's got the costs down an order of magnitude below Amazon.

Using his Altcoin software – you can walk across a border, buy a new a blank computer, type in your 12 word seed phrase, and it will automatically download your entire filesystem (to that computer). It's really kind of cool.

Again, I gave this talk in June, 5 months ago. But I looked up the new numbers, yesterday ~slide~ and here they are. They're up a lot.

Unfortunately, you don't often hear about projects like this, because *99-plus* percent of Altcoins are scams, and it drowns out the useful projects. Which is sad. Yet another thing solved by Bip300, since no scammer would make a Bip300 sidechain.

~ P1 – Ossify Bitcoin Layer1 ~

I will mention that, as an added bonus, if miners upgraded to activate Bips 300+301, then --- theoretically--- that might be the very last time anyone ever needs to upgrade their Bitcoin software again, ever. Which is more convenient, but also more secure as well. (If you're worrying about protecting Layer 1.)

Furthermore, in my opinion, Bip300 is the only practical way of eventually forking the Layer1 Blocksize *down* to 350k, which I know at least some of claim to want. Because this would improve decentralization (as recommended by some experts, including Luke Dashjr).

~slide~ Ok now for those *drawbacks*.

Here they are. The first supposed drawback of Bip300, is that miners can ---with a little bit of setup and technical knowledge and effort on their part, and certainly patience--- miners can remove all the coins from a Bip300 sidechain, and pay those coins, to themselves. Hence it is called the "miners-can-steal" problem. Here you see an evil miner, replacing that one hash I mentioned before with a different hash, and then it eventually pays out (to the miner).

The second, supposed drawback of Bip300, *sigh* is: if some miners ever have a profitable side-hustle, then *maybe* some other miners *might not be **able** to* have that side hustle. And then they might go out of business; and wouldn't be able to buy as many Xmas presents for their children.

~slide~ Both of these are so, false, that its hard to know where to begin.

~slide~ So, Bip300 is designed, to prevent miners from stealing from sidechains. But, it is nonetheless possible. Similarly, – miners "can" (can in quotes **) steal from the LN. In fact its much easier for miners to steal from the LN, since Bip300 has this 6 month timeout period. So, were you worried about miners stealing from the lightning network a moment ago? If so, just cross off this entire left half of the page. I have to stress: this comparison isn't to knock the LN, I'm saying that the criterion is stupid. 51% hashrate can do a lot of horrible things, but that doesn't stop us from ***allowing users*** to opt-in to certain tradeoffs. After all, its Bitcoin not Prison.

The second one is even sillier. I think what I would like to highlight is that the implications are ridiculous. So, if BitFury sold t-shirts on the side, for profit, then *t-shirts = bad for BTC*. They would be as bad for Bitcoin as Bip300 is, anyway. If Michal Saylor altruistically paid miners $0.10 per year, then MS = bad for

Bitcoin. Blah blah blah… I think what's really happening here, is that people are confusing nodes with miners. Miners run nodes, but not the other way around. We want nodes to be as cheap as possible. That is absolutely important; but we don't want mining to be as cheap as possible. If we wanted that, we could just get rid of all of the upward difficulty adjustments.

So I have total contempt for these two supposed drawbacks. In fact both of them are not drawbacks at all -- ~slide~ -- the left one allows for super-reliable oracle and high-quality smart contracts, and the right one is the only thing that is going to keep hashrate security up, in the future. So, they're not drawbacks at all, in fact they're both pretty f**king cool, features.

~How to Get It~

Ok, what should you do? Here is what I suggest:

The most important thing is, to learn. The best way to learn, is to actually download the software and use it. Don't listen to what people say on Twitter. Run the testnet software yourself … otherwise you know … *nothing*.

Second: the Bitcoin community prides itself on consensus – we don't make a change, until lots of people agree that they want it. So: help spread the word. So, talk to your friends or whatever.

Finally, maybe (?) this might help – Change the way you view Altcoins. They aren't rivals, that are inherently evil; they're a place where technology is previewed, before it is copied into BTC.

~slide~

Ok that's the talk, thank you! :)