~title slide ~

Okay, hello. I've been asked 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".

~image – Ver, Vitalik, OLeary~ 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 cover three aspects of the idea. They are Full Autonomy ; Protect the Base Layer ; and Improve Miner Incentives.

Before continuing, though, 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 (that regular people can use, we even have Windows versions now), and there's even a YouTube video of me, using Bip300 on testnet, to copy the zCash Altcoin. So the software can be downloaded and is very use-able.

Ok now back to the three aspects.

~1~ Okay, aspect one: full autonomy. Each 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, Segwit (if they wanted to), 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.

The only constraint imposed on Bip300 sidechains, is that they respect the 21 M coin limit. So, the your projects starts with zero Bit-*coins* on them.

~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).

~slide~ here you see the coins move over. And, by comparison, the Altcoins do NOT move over.

~2 ~

Ok, this is going to be mega-abridged for simplicity.

The point of these next two slides is to show you that an evil sidechain can't cause problems on the base layer. Will it make any sense (?), I don't know but I'm going to give it a try!

So there are two blockchains here; the squares are block headers, and the trailing rectangles are the list of transactions in each block. And time is flowing from left to right. And even though there would normally be tens of thousands of blocks in this period, that wouldn't have *FIT on the* slides so instead there are only seventeen blocks on Layer1 (in blue), and seventeen blocks above, on Layer2 (in red).

~add in the green hashes~

Ok now in green I've added some things. Three months of sidechain activity is compressed into one little 64-character string here. And that string is inserted into Layer1. Bip300 operates entirely off of this little string. (!) Plus a lot of logic.

Therefore, full nodes (on Layer1) do not check anything that is happening on the sidechain (where there can be, theoretically, unlimited complexity – that you aren't checking). The sidechain doesn't need to be a blockchain, it doesn't need to be written in c++, it doesn't need to be decentralized. Bitcoin full nodes (below) won't have any idea what's going on, on layer2, and they won't care. Hence my point: they *can't be harmed* by layer2 because they aren't looking at it. Bip300 just looks at this little hash and does very simple calculations on it, like addition and subtraction. That will tell Layer1 who wants their coins back. And the hash is inside a layer1 transaction, which your full node has to look at *anyway* (specifically, its in the coinbase transaction, if you were wondering).

…[pause] … The two aspects combine and make this "cool A-symmetry". Pay attention because this is important. Users (that's you), ;; can move coins among these networks immediately and trustlessly – using the same HTLCs that are in the LN (they just wouldn't be super fast ones). So if you use Bip300 as intended, its quick and easy. ;;; But in order for anything to go wrong, something very *difficult* has to happen. [gesture] What needs to happen is that a majority hashrate would have to attack the upper network for *at least* 3 consecutive months – 100% of the blocks mis-behaving (or whatever you want to call it). For three month's consecutively, every block. Or 6 months if they do it halfheartedly. So it's very A-symmetric. Very easy to use it right, very hard to use it wrong.

~3~ Okay third aspect. 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, *users* already weren't paying attention, now miners can also ignore Sidechains (if they want). They *still* collect all of the transaction fee-revenues from the sidechain's txn! How does that work? Well, I don't have enough time to explain it to you. But the design is that: if miners just do what they normally do, and include the set of txns, on Layer1 that pay the highest fee, (to them), which is exactly what they already do today, then they will automatically mine all sidechain blocks and collect revenue from their transactions. Even today this would boost fee-revenues by at least 10x, but ultimately I think it could boost fees by 1000x or even more. But I don't have time to tell you about it. I did write an article "Security Budget in the Long Run" that you can look up if you want.

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

~ Possibilities ~ Ok, that was the idea. But what are some concrete use-cases? Well, here are some Altcoins I think we should consider ripping-off.

~zcash slide~ Obviously, zCash I mentioned already. 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. Similarly…

~Monero only~ …there is a darknet market that, a few months ago –*apparently*--- 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. …

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 an article ~slide~ a few months ago –"BitNames, there's the url", and I will now give you a *FEW* of the images from that article. And maybe you can read more about it 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 he wouldn't have to do that at all, everyone would know that he has just the one name.

~BitAssets~ – Ok lets talk about digital assets, now. Erc20/NFTs; People like tokens, even just for fun. … It *is* fun, to collect things. Most NFTs are on Ethereum, which is really lame. If we had Bip300, we could have a whole, ERC20 chain or something.

~ Sia~

This is David Vorick's project (who some of you may know). (Decentralized P2P cloud storage, managed and enforced by the blockchain); It's been running for 5 years, it would keep running if everyone quit. "1TB of storage = $2 a month or less (on Amazon S3 ,that costs $23)"; Using his Altcoin software – you can sit at a blank computer, type in your seed phrase, and it will automatically download your entire filesystem (to that computer). It's really kind of cool. Unfortunately, you don't 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.

~prediction markets~ This is my own project. My other project. I designed to be a Bitcoin sidechain, from the very beginning, but if Bip300 never activates, it will have to be an Altcoin, which is the worst! Anyway please give this other project a look, if you can -- BitcoinHivemind.com, I'm very passionate about it. Here are some screenshots. This software can do a lot of things, but a 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 vote for them.

~ P1 – Ossify Bitcoin Layer1 ~

On top of all that, we might choose to intentionally never change Layer1 again. This would have a lot of benefits.

* * SegWit/Taproot/SH_noInput could be done on its own layer2, basically immediately, with no hassle.

* * No "drama". Right now, there are people who's job it is to decide: which software changes make it into Bitcoin, and which don't. And its horrible, thankless, stressful work, because people (laugh) have very strong feelings about that kind of thing, and so the process is very Dramatic. (to say the least). But with Bip300, anyone can make their own Layer2 blockchain. Then people can go back to just working on the ideas that *they* like, not participating in drama.

* * There's also a problem that today's upgrades are basically mob rule. I don't want to get into the sordid details but, when people advocate on Twitter for like, some soft fork, or another, its very obvious that 99% of them have no clue what their talking about at all. And most of them are just reacting to peer pressure. Which is not going to work in the long run! We've gotten away with it for now, but it's a stupid idea.

* * Final thought, before the very last slide: if BIp300 pans out, and works, then Bitcoiners will be able to use block-space on other blockchains. So we won't need as much layer1 block space. We could very easily soft fork the Layer1 Blocksize *down* to 350k, which would improve decentralization as recommended by some experts.

Anyway, that's the idea, last slide..

~How to Get It~

If you want to get Bip300 faster, then 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. And then talk to other people about your experience We have software with a GUI.

Also, 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.

Ok that's the talk thanks :)

Also, so you have to wait for me to finish it.

In general just focus on the idea of *abundant, freely-programmable* blockspace; and open competition among developers with *no barriers to entry.* One developer could singlehandedly change everything. That’s what we want – we want all the developers to be working overtime to try to change the world and make each other envious. Now, its too bureaucratic and slow, in my opinion. Greg Maxwell could just veto a change he doesn’t like, or Wladimir. Instead we want some 15 year old out there to say, “you know what – I’m going to be the next [big person] or whatever and I’ll do it by myself, in my own way”. That’s what we want.

Which brings me to my next point.

3. Always Insist on ***Your*** Sovereignty

Who decides what apps run on your phone? …you, or some bureaucrat?

~Mistaken Cultural Beliefs that Slow Down Adoption of Bip300~

Ok. Now I have a section called

These are beliefs that , are false, and harm Bitcoin. So if you want Bip300 you have to make sure that you push back against them.

~Two Natural Enemies~

1. The Pump&Dump Altcoin Scammers

- The ***whole existence*** of Altcoins, the entire sales pitch, ***needs*** it to be the case that there are things that BTC can't do. But if BTC can do anything, then why should anyone buy an Altcoin?

2. The Self-Appointed "Defenders of Bitcoin" – the people who keep bad ideas out of layer1.

The first is straightforward – obviously, if there's no longer any need for Altcoins, then scammers can't shill an Altcoin, and trick people into buying it. The second is more nefarious – right now there are people who decide, what should-or-should-not be in the Bitcoin protocol. And those people are also out of a job, if BIp300 activates.

This, proposal, does their job, better than they ever could! It puts the out of a job. They are like the regulators, doing regulatory capture.

Enemies of bip300 – people who proposed rival ideas and who are jealous,

---

~timeline~

This is a very old idea. I won't go through the entire history, but I wanted to give you an idea of just how many people have touched the idea. It's very old

~Not Vaporware!~ ~screenshots of Github, GUI, Youtube video~

I also wanted to give you a slide that shows you

the code on Github; a software release with a nice GUI; and a Youtube video of us sending coins to a zCash sidechain , and taking them back.

This idea is very difficult to understand … apparently. Definitely, it sounds too good to be true, at times.

[pause]

But it is true, and in fact I have some since screenshots for you of:

So: people don't think it can be done, even though it ***has already been*** done.

~not a shmuck~ ~list of credentials~

And who am I? Well, before I continue, I have a slide designed to convince you that I'm not a ***complete*** shmuck.

From 2012-2015 I was a statistician at the Yale department of economics, In Aug 2015 I wrote an anti-PoS essay called “Nothing is cheaper than proof of work” that is sort of quasi-famous (to this day). In January 2014 I wrote a paper called “truthcoin” that inspired / defacto-created an entire generation of oracle/prediction-market projects, I presented at the first three scaling conferences and was on the program committee for the fourth. (The scaling conferences failed to prevent the Blocksize civil war so I completely lost interest in them after that.)

Beyond Peer Review

This project handles changes to Bitcoin’s software, via hardcoded protocol rules. It naturally competes with the people

~Nick Szabo essay~

It also reduces their status – as, currently, they are irreplaceable elites upon which we rely, whereas if Bip300 activates there kind of would be no such thing as a Bitcoin developer. Right know they – or perhaps I should say “we” – have a monopoly, but if Bip300 activates, development will become competitive. No one will be able to veto an idea or erect any kind of barrier-to-entry that exists now.

Developers brooding responsibility

TSA – “This is for your protection!”

- Must let the developers off the hook.
    - Currently: they feel responsible
    - Get a lot of praise/money/autonomy/fame in return.
- Many people do not want to be responsible

- Currently: people play it safe and “trust the experts”
- People would have to be more comfortable taking their own risks.

If people are

~largeblock sidechains (BCH)~ Here’s another idea, what about large block sizes? Oh noo…. Like BCH? Bcash? Everyone hates that, right? Don’t worry I put it second-to-last, so that it would be the most forgettable. Ok, well, large blocksizes might be a bad idea on layer1 … but they are potentially a good idea on layer2… because Layer2 is ***optional***. Also, layer1 is existential, but Layer2 can be paused and resumed later. Kind of like a motte-and-bailey strategy, as I presented at Scaling 3. The bad guys come you hid in Layer1 bunker, then when the bad guys leave you go back to Layer2. The benefits of a Bip300 largeblock sidechain are pretty clear: First -- accommodate very many users, very quickly. (~slide~) Two, the resulting payments network would *just look* a little more like the existing world’s payments system, which I think is always a good sign. Three -- not every transaction requires the same level of decentralization -- if you want to achieve 100% Bitcoin dominance, you have to keep that kind of thing in mind (I mean, how do we beat the centralized Altcoins? Do we just preach at them? Better to at least be able to play as dirty as they do, maybe). Fourth, the networks world organize themselves geographically, just, automatically; but the full nodes of one network could live in a different political jurisdiction (than their users). Which has interesting implications. You’ll have to read my post ~slide~ if you want to learn more about what I mean.