~Title~

~Hello ~

Hello, my name is Paul Sztorc. I have been a Bitcoiner since 2012. And I've published Bitcoin research, on my blog "truthcoin.info" since 2014. I presented at many Bitcoin conferences, especially the scaling conferences, as well as Building on Bitcoin (last summer) and TABConf earlier this year. I currently work for Tierion as a research director. Before that, I worked a kind of pre-doctoral research statistician job at Yale for 2 years for a man named William Nordhaus, won the Nobel Prize in economics a few months ago.

~topic~

The topic of this presentation, is a Bitcoin layer-2 solution called Drivechain. These days I'm calling it a layer-1.5 solution, because it sneaks in between layer-1 and the Lightning Network. (And everyone's calling Lightning layer-2 -- and Lightning can go on top of this! So it has to fit in between.). 1.5 is also appropriate, because each Drivechain is a layer-2 of BTC, but they are also a layer-1 of their own blockchain. (So it's kind of like "are they a layer-1 or not?" …well, they're a 1.5).

Drivechain aims to provide scalability and interoperability, and can be deployed via soft fork. It's very slowly being assigned the BIP numbers 300 and 301, and the project website is drivechain.info . If you are technical, I recommend you read the BIPs, otherwise I would recommend browsing drivechain.info – there's tons of information there.

~in one slide~

Here's the talk in one slide:

Problem – **Meta-Consensus (ie, Altcoins, Hard Forks, and Contentious Features)**

Consensus: getting all nodes to look the same way. And we know how to do that. Meta-Consensus: Humans agreeing on ….what those nodes should be agreeing about. Its consensus-about-consensus – for example, the Blocksize debate, but also SegWit and checklocktime verify, and every other consensus

change to Bitcoin. And every hypothetical change to Bitcoin, turing complete scripts, mimblewimble, whatever.

We know how to get nodes to agree with each other – we know consensus. But we don't know what to do, when we humans disagree about what nodes should be doing. When that happens we get Altcoins and Hard forks , or we miss out on good features (maybe).

Solution – one token, traveling among many blockchains

This idea used to be called "sidechains". But that word has almost no meaning today – it is now used to describe, even things that are not blockchains at all. (Let alone what the word originally meant, was a very specific and new type of blockchain). So the word "sidechain" probably just causes confusion at this point.

In a sentence: why settle for the best features (Bitcoin Core), when instead you can have every feature? Why compete to win, when you can play all the hands? (And then you can't lose).

~How it works~

The soft fork allows a new kind of output, called a "hashrate escrow". Anyone can put BTC into it; but money can only be taken out of it by miners, who can send it wherever they want. But they can only extract it very slowly and transparently. So instead of paying money *to* a person, you put it into this –sort of— process.

~Prison Metaphor~

Metaphorically, the escrows are kind of like prisons where miners are the warden. You can choose to go in, at any time, but then its hard to get out.

~Prison = a pentagon with a long channel of gates~

~Example~

I realize that explanation probably made no sense, so here is an example.

1. We start with one blockchain – that's Bitcoin Core.
2. Bitcoin Core soft forks to add Drivechain – specifically, it adds BIPs 300 and 301.

---the guy who does all of the real work on the project, CryptAxe, loves qt and he made all these themes for Bitcoin in his spare time—so as a bonus you get GUI themes --

3. Roger Ver disagrees with the consensus rules of Bitcoin Core, specifically the 1 MB Blocksize limit.
4. Roger Ver hunts around for like-minded people. They form a new community; and they create a new blockchain --using our template-- that has the consensus rules that they want.

--Now, this template is a different piece of software than [what you just saw], Core + BIP 300/301. Pay attention to the circles -- the first software is specialized to have multiple "hashrate escrows", we still call them "sidechains", and the template is specialized to have one "parent chain".

[4b] Roger and Friends call their new software "Bitcoin Payments". As with Lightning (and other layer-2s), "Bitcoin Payments" is always watching Bitcoin Core, and it requires a Bitcoin Core full node.

5. Next, Roger and friends add a new hashrate escrow –a new prison— on Bitcoin Core, and tie this "escrow" to their new Payments chain. (Maybe you can see, there's fields for that).
6. Roger sends 50,000 of his BTC from layer-1 ("Bitcoin Core") into this prison ("Bitcoin Payments"). Over in Bitcoin Payments, he gets credited for it. ~slide~ And so do some other people. You can see all the BTC gets crunched into this output up here, on layer-1. These transactions are unremarkable – just like spending to a SegWit output or a P2SH output. Going *into* prison is – as easy as doing anything else. *Leaving* prison is where it gets weird.

7. Roger goes all around the world, giving away free Bitcoin, and convincing people to download the Bitcoin.com wallet. But when he gives away Bitcoin, it is always on layer-1.5, it is always within the prison. Nothing is happening on Layer-1. So onboarding is actually very easier. Now, this is important: --the transactions in the prison don't show up on layer-1, but their transaction fees do show up on layer-1 due to something called Blind Merged Mining. 20 minutes isn't enough time to explain both, but in one sentence I'll just say that the act of finding a merged mined block [ie, tracking what happens in the prison] , that is transformed, into the act of including a single layer-1 txn.
8. When laypeople –that's you guys in the audience-- want to settle their coins back to layer-1. Laypeople want to leave prison. You use atomic swaps, or they use a service like ShapeShift, or SideShift. Sideshift charges 1%, but you get out of prison immediately— ~slide~ its like a prisoner exchange, you sign over the incarcerated coins to someone else, and you get layer-1 coins. The total network cost is one layer-1 txn and one layer-1.5 txn. So, up top, you can see that something has happened on layer-1.
9. Of course, eventually Andreas Brekken (leader of Sideshift), and Erik Voorhees (leader of ShapeShift) are bag-holding a ton of escrowed coins! They made 1%, but they're in prison. And they want to get out. So how do ***they*** do it? On Bitcoin Payments, they submit withdrawal messages. Those are the speech bubbles.
10. The Bitcoin Payments Full Node (the new one) assembles all of these requests, and defines a single transaction that can fulfill all of them. ~From BPayments, to EV, AB, 1, 2,3 etc~ And this transaction can be summarized by 32-bytes. These 32 bytes are broadcast by BPayments full nodes and BPayments SPV nodes. ~slide~ You can see here that we've run getblockheader, in the template. This example has a bunch of zeros in it, but if there were withdrawal-requests,

then this is where these 32 bytes would be. They'd be in every header of every Bitcoin Payments block for as long as it takes – until the withdrawal either goes through, or until it fails.

11. A Bitcoin Core miner sends a coinbase message with these 32 bytes into the first gate here.
12. In the next block, it either moves forward a gate, back a gate, or stays where it is. (Oversimplified) Miners control which direction the bytes move.
13. Over the next 3-6 months, if these bytes make it to the last gate, the 13,150th gate, then txn matching that ID can be included on layer-1, and the funds can be withdrawn from prison. Erik and Andreas are happy, everyone is happy.

~Costs and Risks~

Now, before I go any further, let's talk about the costs and risks of that idea. All the bad news first. So you can decide if you even think this idea is worth learning about.

Any funds sent into an upper layer, have to deal with the new security considerations of that layer.

~Upper Layers~

For example, in the Lightning Network, you have new things to worry about. You need to be able to notice fraud quickly (possibly by relying on watchtowers); you need to be able to broadcast a layer-1 txn, in time to prevent any theft, *of your coins*, (and you need that, to be economical); you need to be able to wait out the custodial period if your counterparty goes AWOL.

In Drivechain, you also have something new to worry about. ~slide~ And it is this: are these esrows (the prisons) adding value for miners, (especially the escrow you are using)? So if Drivechain is a popular feature in general, then you'll be comfortable. The escrows will be boosting the value of BTC, and contributing a lot of transaction fees -- and so miners will want the escrows around.

If miners don't want the Escrow around, they can withdraw all of its BTC to themselves:

~Miner Theft~

1. First, they figure out exactly how to divide it amongst themselves. In this case I've given it all to Jihan Wu.
2. They calculate the 32 bytes that would correspond to this transaction.
3. They will put these 32-bytes into the first gate.
4. All users of the L1.5 software will know immediately. And, because of twitter/reddit, everyone else will know soon afterward. This includes:
    a. People who want to point and laugh. ..but it also includes…
    b. People use *other* L1.5s and are concerned that they'll be the next victims.
    c. And it also includes people who have never used L1.5 for anything, but who were planning to make use of them some time in the future.

~3 months~

5. Then, 3 extremely awkward months follow. Assuming there is 100% hashrate behind the attack --because remember the 32-bytes can be sent back a gate, as well as moved forward. They only move one gate per 10 minutes. So if some miners aren't attacking, it might be 6 awkward months before the bytes finally make it out.
6. All 50,000 of the BTC that Roger originally deposited to the escrow, now goes to Jihan Wu. The fact that Roger maybe sent it to 10,000 people in the meanwhile doesn't matter. Layer-1 has no idea what happened on layer-2, if anything.

So that's the bad news.

~Summary~

In summary, the idea boils down to this:

1. Create new blockchains for people to use. If people use them, then this adds value to miners. Both *directly* in the form of more transaction fees, but also *indirectly* (because a BTC that can do anything, should be more valuable than a BTC that can do only one thing).
2. Give miners the choice, of taking this revenue, or leaving it.
3. Make the system extremely-auditable, by:
    a. Reducing all the economic activity inside the prison down to only its net transfers.
    b. Crunching all transfers down, to 32 bytes.
    c. Only allowing one transfer at a time.
    d. Transfers take 3 months to settle.

~Good News~

The good news is that, like all upper layers, if you don't want to ***use*** this idea, you don't have to. *Now*, to be a full node, you *do* have to check all the rules. Bitcoin Core –after the softfork—would need keep track of how many prisons there are, and where each 32 byte withdrawal is, in its series of gates. So, there is a tiny amount of full node overhead, but in principle this is no different from CheckLockTime Verify or CheckSequence Verify or the requirement that Coinbase-txns contain block-heights. No different than what we've done a dozen times already. And than what we plan to do many times in the future.

For some reason, it is believed, especially among two people in particular, that mainchain users, or miners, are required to interact with the upper layers. But they aren't – everything required, to fully validate layer-1, is right there in layer-1. It isn't in any of the other layers. Furthermore, everything that miners need, in order to collect all of the transaction fees from each upper blockchain (Bitcoin Payment,

for example), is also on layer-1. You have to read BIP 301 to understand why. All miners are doing is including valid layer-1 transactions, in layer-1 blocks, which is the same thing they have always done.

~LN vs Payments Chain~

Now, I will take the hypothetical "Bitcoin Payment" escrow (from our example above), and compare it to the beloved Lightning Network. Here I've outlined the process for (#1) onboarding a new user, (#2) making N payments, and finally (#3) settling your net wealth to layer-1 cold storage. …To try to make it apples-to-apples.

~Network Costs~

And, assuming that process, I have tabulated total network txn fees, for each. The Lightning Network charges a %-based fee for payments, as will ShapeShift/SideShift. LN pays more of these fees, n of them, and more of the Layer-1 transaction fees (which obviously will be much more expensive, per txn, than layer-1.5 txn fees).

This comparison suggests, that the Lighting Network will be cheaper when the magnitude of payments is very low, and when the absolute quantity of payments is very high. In other words, LN will be cheaper for micropayments. … Otherwise, the payment sidechain is cheaper.

~user experience~

I have also tabulated the *user experience*, for each system. I'm assuming that the user is willing to swallow that new security consideration -- in other words, I'm assuming that the Payments Sidechain is popular, and that miners like having it around. (raise finger) Certainly, not everyone will be comfortable with that new assumption. But many people probably will be, and they inherit a lot of advantages that are worth talking about. In particular, you can get onboarded without a Layer-1

payment, and you can receive money when you are *offline* or *asleep* or *separated from your private keys* or *in a coma* or whatever.

…these other ones are maybe not as important. The main LN advantage is that it should give you a pretty decent amount of *finality* immediately. When buyer and seller are face-to-face, in person, they've both got their phones, then Lightning Network is probably much better.

~Other Benefits~

Ok here's the thing. While the Payments sidechain does make a pretty decent Drivechain example …for a tiny 20 minute talk… ***scalability*** is not the primary purpose of Drivechain. At all.

~Goals~

These are the real goals:

1. Neutralize Threats --- (Altcoins / Hard Forks)

    SegWit2x being a perfect example – it was proposed right here at Consensus, two years ago. Instead of doing a social media campaign , you just let them spin off their own chain. Remember, it doesn't matter how bad the idea is – if it gets adoption it is a potential threat.

2. Boost txn fee revenues. This ensures hashrate security in the long run.

Currently, txn fees totaled $70 million last year – a microscopic number. In my opinion, they eventually need to be at least four orders of magnitude higher – 10,000x higher, so we're nowhere close. Unfortunately, if Bitcoin has competitors, then it is unclear how that $70 million number will increase at all. Even if you think Altcoins are dumb, --you're almost certainly right—what if someone just makes an exact copy of BTC, purely to create some new block space. That would have to be a decent competitor to BTC if you like BTC. Instead of one winning BTC chain, we would just have a cluster of

wining BTC chains, and whenever layer-1 fees rose, it would just stimulate the creation of new competitors. But they'd all have low fee rates, low total fee revenues, and insecure hashrate. But with this all of the fees on all of the chains go to the same miners.

…

3. Bring Cool New Projects to BTC

Ok, what new projects does BTC need? Isn't it already perfect?

Well I just explained the Payments Escrow idea. And even if you are a hardcore maximalist, you probably support Blockstream's Liquid network, which adds extra cryptographic privacy, and the ability to issue custom bit-assets. You want improvements over time – Schnorr, taproot, graftroot, signhash_noinput, etc. – now, those are softfork-able. But that's not true for MimbleWimble, or Turing Complete scripts. Its not true for a lot of things.

~Hivemind~

Specifically, I have another project, which is my primary focus, not this. It is at BitcoinHivemind.com , and here are some endorsements of it. I hate to rely on endorsements, but I don't really have time to explain the project itself. There are great videos that do that, on the website. Go there and watch them.

~Toxicity~

In General, I do think the space would be more fun to work in, as well, and be more productive, if we had something like this. But I don't really have time to explain why.

Ok, that's the talk, thank you!