PlanB Forum Lugano: a great experience

These days at PlanB in Lugano were incredibly stimulating and exciting.

I presented my ideas to people like Adam Back (Blockstream), Jameson Lopp (Casa), Samson Mow (Jan3), Giacomo Zucco (LNP/BP association), Federico Tenga (RGB), Allen Farrington (investor), Rahim Taghizadega (Scholarium), and many many others.

Although I already personally knew a few of them, I must admit that the Bitcoin community is made of some great personalities, open minded and humble, despite their fame, social status and intelligence. I asked Adam if he was available for 10 minutes, but then we talked for more than 1 hour. He was so available and kind.

Talking with such a key person in the invention of Bitcoin is thrilling. Before, I never had a "in depth" conversation like that with a person of his caliber, especially about my ideas regarding sidechains, scalability, consensus systems. Therefore, this discussion for me was an honor and joy and, somehow, also a relief. In fact, until you don't go through it, the doubt remains that people with more knowledge and experience than you could destroy your theories in a fraction of a second.

It seems that there are some fundamental things on which Adam agrees with me, like the congestion that may come from the **intensive use of Bitcoin UTXO** (for purposes that are different from Bitcoin payments, like asset tokenization), which may lead to the concept of a sidechain. But not only that.

Adam expressly recognizes that **the peg-in is a centralizing force in Liquid**, for obvious reasons: if the federation is

malicious, the entire value of the sidechain is lost. Also, I think he is genuinely interested in a “peg-less” sidechain and in the idea of “improved” cross-chain consistency given by the anchoring to the slavechain, although he didn’t express it explicitly.

However, I had the impression that he thinks the centralizing aspect of Liquid is the peg-in only, not the block issuance. He doesn’t seem concerned about the block issuance governed by a close federation of 15 entities. He said **it’s also possible to have a single blocksigner.** After all, nodes can realize if the consensus is broken and they can hard fork and replace that single blocksigner. The state of the blockchain is never lost. The important thing is that there are node validators that can check if the consensus is broken – he said.

Since such a hard fork would require manual intervention, I pointed out that a single blocksigner acting maliciously only once may destroy the trust in the system forever. I illustrated what I am envisioning as a **replacement for the Strong federation model**. He told me he didn’t know much of Algorand’s cryptographic sortition and I summarized it briefly.

You can expect the inventor of the Proof of Work remains quite skeptical about the Proof of Stake, but he has a point: PoS systems are complex. **Any complex system introduces many risks**. At least, a federation is simple and predictable: if the functionaries are honest, it works well, if they are dishonest or corrupted, users must hard fork and replace them. He somehow suggested that it might not be necessary to rely on a PoS if we want an alternative to the Liquid federation, there are various protocols and experiment out there and he suggested that I could take a look at other Bitcoin projects (I think he mentioned Fedimint, Fabric, Counterparty and a few others) to find out if there is something to be inspired by that could grant the same model of immediate transaction finality I am looking for.

I still remain of the idea that opening the “federation” to the free market, rather than trying other permissioned or semi-permissioned protocols, is the ideal path to follow. However, I will certainly treasure his advice, looking at all project he mentioned, and of course, we will be as cautious as possible implementing the PoS on top of Elements, trying to detect any new potential vector of attacks.

I think that **the free market for transaction fees** was interesting to him, he actually started brainstorming and thinking out loud about that. For example, he tried to imagine if there was the possibility to have a minimum fee by default, somehow anchored to the value of a particular coin or peg, as an anti-spam measure without relying on the blocksigners’ will. Of course, this would result in the centralization towards a single peg or asset, so he discarded this idea. Obviously, I was ahead of him in this topic since I already thought about these things for a long time, but it was nice to see how quickly he was processing and discarding those ideas and coming to my same conclusions.

He also started giving suggestions on how to develop Sequentia and also its DEX. Finally, he somehow seemed to “apologize” for not having Liquid and Elements so “open” and available to anybody as it would be possible. He told me that Blockstream will publish the code that is currently not open source regarding the communication between the functionaries. He was just thinking out loud, since after one second he said “well, actually you may not use that, since you are replacing that part with a different consensus”. However, it was nice to hear those things because I could realize how transparent he was and I enjoyed that his thoughts were freely flowing to me. Above all, I loved that he was truly concerned about the fact that he wasn’t helping “the rest of the world” (like me) in all the possible ways he could. I realized how really “good” he is as a person, not only as a scientist, and how he truly loves the world in an altruistic way.

Thank you Adam! And he is just one of the many great people I interacted with in Lugano! Bitcoiners are amazing

Ps: in this summary of the conversation I had with Adam I hope I haven’t misrepresented any of his words. I tried to summarize here objectively and not distorted by my own perception, but keep in mind he hasn’t viewed or in any way “validated” this summary