PlanB Forum Lugano: un’esperienza meravigliosa

Questi giorni a PlanB hanno rappresentato forse il momento più entusiasmante per la mia “vita da Bitcoiner”.

Ho presentato le mie idee a persone come Adam Back (Blockstream), Jameson Lopp (Casa), Samson Mow (Jan3), Giacomo Zucco (LNP/BP association), Federico Tenga (RGB), Allen Farrington (investor), Rahim Taghizadega (Scholarium), e molti molti altri.

Anche se conoscevo già alcuni di loro, devo ammettere che la community Bitcoin è fatta di alcune personalità incredibili, open-mind, umili, a dispetto di fama, affermazione nel settore e, soprattutto, intelligenza. Ho chiesto ad Adam se avesse 10 minuti per me, alla fine abbiamo parlato oltre 1 ora. È stato sorprendentemente gentile e disponibile.

Parlare con personalità che sono state fondamentali per l’invenzione di Bitcoin è stato emozionante, non avevo mai avuto una conversazione così approfondita con persone di quel calibro, specialmente non riguardo a sidechain, scalabilità e sistemi di consenso. PlanB è stato per me gioia, onore e, tutto sommato, anche sollievo, se vogliamo. Infatti, finché non affronti a viso aperto persone di quel calibro, i dubbi rimangono che persone di quel calibro, con la loro conoscenza ed esperienza, possano distruggere tutte le tue teorie e aspettative nella frazione di un secondo.

Sembra che ci siano alcuni temi fondamentali su cui io e Adam concordiamo, come la congestione che può derivare da un uso intensivo degli UTXO Bitcoin (per scopi diversi dai pagamenti Bitcoin, come la tokenizzazione di assets), i quali sembrano condurre naturalmente ad un’idea di sidechain. Ma non è tutto qui.

Adam riconosce espressamente che il peg-in è una forza centralizzante in Liquid, per ragioni ovvie: se la federazione è malevola, l'intero valore della sidechain è perduto. Inoltre, penso che sia genuinamente interessato all'idea di "peg-less" sidechain e ad un miglioramento dell'affidabilità delle operazioni "cross-chain" data al modello di slavechain grazie all'ancoraggio, sebbene non l'abbia espresso esplicitamente.

Tuttavia, ho avuto l'impressione che lui ritenga che l'aspetto centralizzante di Liquid è esclusivamente il peg-in, non l'emissione dei blocchi. Non sembra preoccupato del fatto che la produzione dei blocchi sia governata da una federazione chiusa di 15 entità. Ha anche detto che è possibile avere un singolo blocksigner. Dopotutto, i nodi possono sempre rendersi conto di quando il Consensus è "infranto" e possono fare hard fork, rimpiazzando quel singolo blocksigner. Lo "stato" della blockchain non è mai perduto. La cosa importante è che i nodi validatori possano controllare queste rotture del Consensus – riporta Adam.

Dal momento che siffatto hard fork richiederebbe un intervento manuale, ho sottolineato che se tale "singolo" blocksigner agisse mai in modo malevolevo, potrebbe distruggere per sempre la fiducia che gli utenti ripongono nel modello. Ho in seguito illustrato la mia visione per rimpiazzare il modello di Strong federation. Adam mi ha detto che non conosce bene nei dettagli la cryptographic sortition di Algorand, perciò gliel'ho riassunta in breve.

Vi potete aspettare che l'inventore della Proof of Work rimanga piuttosto scettico relativamente a una Proof of Stake, ma ha le sue ragioni: i sistemi PoS sono complessi. Ogni sistema complesso introduce dei rischi. Almeno, una federazione è semplice e prevedibile. Se i funzionari sono onesti, funziona bene, se sono disonesti o corrotti, gli utenti devono fare hard fork e rimpiazzarli. In qualche modo, Adam sembrava suggerirmi che non dovessi necessariamente

affidarmi a un PoS se voglio trovare un'alternativa al modello di federazione di Liquid, vi sono vari protocolli ed esperimenti fra i vari progetti Bitcoin che potrei analizzare (mi sembra che abbia menzionato Fedimint, Fabric, Counterparty e qualche altro) al fine di vedere se potessi trovare l'ispirazione per un modello che garantisse la stessa transaction finality immediata che vado cercando.

Rimango dell'idea che aprire una "federazione" al libero mercato, piuttosto che provare altri protocolli permissioned o semi-permissioned, sia l'obiettivo da perseguire. Tuttavia, farò certamente tesoro dei suoi consigli, guardando ai progetti che ha menzionato e, ovviamente, rimanendo molto cauti nell'implementare un PoS su Elements, cercando di individuare per tempo ogni potenziale vettore di attacco.

Quello che ho trovato veramente piacevole del suo approccio è che non ha mai sottolineato che la presenza di un governance token nel PoS potesse essere un problema in sé, nonostante sia proprio lui a proporre l'idea di "innovazione senza speculazione". Al contrario, ha sempre dibattuto strettamente su un piano accademico e teoretico, mai ideologico.

Ha anche specificato che, almeno per quanto ha visto, gli risulta che un vesting così lungo sui token del team (come nell'allocazione di SEQ) è più comune in progetti che non performano molto bene sul mercato (ha fatto l'esempio di Zcash), suggerendo che la ragione potrebbe essere gli incentivi inferiori per il team nel fare marketing, se si penalizzano troppo con lunghi lock dei propri token. Io ho replicato che il relativo insuccesso di Zcash potrebbe anche derivare dal focus di quel progetto sulla privacy, che non è esattamente la prima attrattiva per le masse. Se il tuo business model è focalizzato sul DEX e altri use case speculativi, è probabilmente diverso.

Penso che il libero mercato delle fee di transazione sia un concetto interessante per Adam, che ha effettivamente iniziato

a fare brainstorming di fronte a me, pensando ad alta voce. Per esempio, ha provato a immaginare se ci fosse la possibilità di avere una fee minima di default, in qualche modo ancorata al valore di un particolare token o peg, come una misura anti-spam senza dover affidarsi alla volontà dei blocksigner. Ovviamente, questo risulterebbe in una centralizzazione verso un singolo peg o asset, perciò ha scartato questa idea. Su questi temi ero comprensibilmente un passo avanti a lui, dal momento che avevo già riflettuto a lungo su di essi, ma è stato bello vedere come processasse velocemente quelle idee e le scartasse, arrivando alle mie stesse conclusioni.

Adam ha quindi detto che io avrei potuto soltanto disattivare il peg-in in Elements e sviluppare l'ancoraggio, ma qui io ho specificato che sviluppare un nuovo consenso non significa necessariamente disattivare il peg-in, soltanto rimuovere il fatto che sia usato nativamente per pagare le fee. Lui quindi ha aggiunto che in un libero mercato delle fee di questo tipo, avere molteplici federazioni che governano i peg-in sarebbe interessante. Ha anche suggerito che potremmo automaticamente fare swap dei token guadagnati dai blocksigner per BTC, e ha menzionato Stacks che ha implementato una cosa di questo tipo. Gli ho risposto che effettivamente avevamo già pensato a questa cosa (proposta da Andreas) e che di sicuro l'avremmo implementata anche su Sequentia.

Ha quindi iniziato a suggerire come sviluppare Sequentia e il suo DEX. Per esempio, anzitutto mi ha linkato un progetto che ha forkato da Elements, per dare un'occhiata a come avessero fatto, poi ha specificato che per i nostri "lightning swaps" fra i BTC sulla mainchain e altri assets della slavechain, potremmo usare C-Lightning, che è già integrato in Elements. Sebbene al momento funzioni soltanto per un singolo asset, ha suggerito che potremmo iniziare con uno solo (Tether) e poi espanderne le funzionalità. Dopotutto, inizialmente, ben pochi assets avranno liquidità sufficiente per viaggiare su

Lightning, probabilmente solo BTC e USDT.

Infine, mi è sembrato che in qualche modo si “scusasse” per non avere messo ancora tutti gli elementi di Liquid alla portata di chiunque. Mi ha detto che Blockstream pubblicherà il codice che attualmente non è open source riguardo alla comunicazione fra i funzionari. Stava solo pensando ad alta voce, infatti un secondo dopo ha aggiunto “beh, effettivamente potreste non usarlo, dal momento che rimpiazzate il modello di consenso, quindi non ti servirà”. Ad ogni modo, è stato bello sentire quelle parole, ho capito quanto trasparente fosse come persona e mi ha fatto piacere che i suoi pensieri fluissero così direttamente a me. Ma soprattutto, ho amato il fatto che sembrasse veramente dispiaciuto del fatto che non stesse aiutando “il resto del mondo” (ad esempio me) in tutti i modi possibili in cui potrebbe farlo. Ho capito quanto “buono” sia come persona, non solo come scienziato, e quanto veramente ami il resto del mondo in maniera altruistica.

Grazie Adam! E lui è solo una delle tante grandissime persone con cui ho interagito a Lugano! I Bitcoiners sono persone incredibili! :)

Ps: in questo riassunto della conversazione che ho avuto con Adam spero di non aver travisato alcuna delle sue parole. Ho provato a riassumerle qui in modo oggettivo e non distorto dalla mia percezione personale, ma specifico che Adam Back non ha letto né “validato” questo mio riassunto